View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Khazar University Institutional Repository

MINISTRY OF EDUCATION OF THE AZERBAIJAN REPUBLIC

KHAZAR UNIVERSITY

SCHOOL OF ENGINEERING AND APPLIED SCINECES

Major : 060631-Computer Engineering

MASTER THESIS

Title: Key pre-distribution protocols in Wireless Sensor Networks using Dominating Sets

Master Student: Farid Nuraliyev

Supervisor: Amir Hassani Karbasi

Baku-2017

Abstract

It is undeniable that networking technologies, especially wireless communications, have changed our everyday life. The innovations in networking technology especially, at the past two decades has resulted in wireless networking capabilities that have changed the way we create, share, and use information. The wireless Internet together with advances of computing and networking technology entered into realityin the information age which should have supposed to be there a long time ago. These information innovations have the effects on global socioeconomic and cultural conditions. These impacts have extremely had a deep consequence on the operations of military forces and governments' secure applications. Timely and reliable access to information is key to the success of virtually all government and military functions. Having effective communications and networking resolutions are critical to the any mission success.

Revitalization in hardware and new conceptions in wireless network technologies have generated low-cost, multi-serviceable small sensor devices. With the help such devices are created hundreds or thousands of ad hoc tiny sensor nodes disperse crosswise a geographical place. Distributed sensor nodes cooperate among themselves to make a sensing network. A sensor network could serve for access to data anytime, anywhere by gathering, proceeding, analyzing and distributing dataand it is extremely efficient in platforms which have prevalent applications for monitoring. So, with the help of such sensor nodes created a smart environment.

WSNs are vulnerable to some damaging attacks. Two by two key pre-distribution design is fundamental for WSNs origin to resource restrictions in the sensor nodes. We will give attention to symmetric design of combinatorial set system which is known as projective plane for illustrating deterministic key pre-distribution to WSNs. Initially a mathematical model is suggested to the networks. Then we design the different applications for wireless network using connected dominating sets. After that for improving projective plane a modern model is suggested which is key copying and exchanging based on CDS and virtual backbone. Results illustrate

that the combinatorial and CDS-based routing approach gives productivity and strong rate for sensor flexibility, optimal resource allocation and scalability in WSNs.

Xülasə

Şəbəkə texnologiyası, xüsusilə də kabelsiz şəbəkə, bizim gündəlik həyatımızda böyük dəyişiklər edib. Son 20 ildə şəbəkə texnologiyasında olan yeniliklər informasiyanın yaradılması, paylaşımı və istifadəsinin üsullarını dəyişməyə imkan verən kabelsiz şəbəkənin yaranması ilə nəticələndi. Lakin hesablama vəşəbəkə texnologiyalarındakabelsiz internetin öz yenilikləri ilə birgə real informasiya erasına daxil olmasi fərziyyəsi 20 ildən dəəvvəl irəli sürülmüşdü. Bu informasiya mübadiləsi yeniliyi qlobal sosial-iqtisadi və mədəni vəziyyətə öz təsirini ciddi şəkildə göstərdi. Bu yeniliklər öz effektivliyini daha dərin olaraq dövlətlərin və hərbi qüvvələrin əməliyyatları zamanı göstərdi. Belə ki, informasiyanı zamanında və rahat şəkildə əldə etmək bütün dövlət və hərbi əməliyyatlarda uğur qazanmanın açarıdır. Effektiv rabitəyə və aydın şəbəkəyə malik olmaq uğur qazanmaq üçün vacibdir.

İT avadanlıqlardavə kabelsiz şəbəkə texnologiyasinda olan irəliləyişlər qurulması az maddiyyat tələb edən, bir neçə vəzifə icra edə bilən və kiçik ölçüyə malik olan sensor qurğuların yaranmasına gətirib çıxardı. Yüzlərlə və ya minlərlə bu cür sensor qurğuların köməyi ilə onlar coğrafi region boyunca sıx şəkildə səpələnir. Səpələnmiş bu qurğular öz aralarında kabelsiz sensor şəbəkə yaradırlar. Sensor şəbəkə istənilən vaxt məlumatı əldə etmək, istənilən yerdə məlumat toplamaq, informasiyanı emal etmək, analiz etmək və məlumatı yaymaq kimi vəzifələrin öhdəsindən gəlir. Bundan əlavə bu şəbəkə geniş yayılmış müşahidə tətbiqetmələrinə malik platformalarda daha səmərəlidir. Beləliklə, belə sensor qurğuların köməyilə ağıllı ətraf mühit yaradılır.

Kabelsiz Sensor Şəbəkələrbəzi dağıdıcı hücumlara qarşı zəifdir.Cüt-cütöncədən açar bölüşdürülməsi texnologiyası sensor qurğularda olan məhdudiyyətlərə görə Kabelsiz Sensor Şəbəkələri üçün fundamentaldır.Biz öz diqqətimizi kombinator çoxluq sisteminin simmetrik dizaynına verəcəyik.Hansı ki, Kabelsiz Sensor Şəbəkə üçün öncədən açar bölüşdürülməsini nümayiş etdirən proyektiv sahə kimi tanınır. Əvvəlcə şəbəkənin bütün xüsusiyyətləri nəzərə alınmaqla riyazi modeli qurulur. Daha sonra rabitəli hakim çoxluqlardan istifadə etməklə kabelsiz şəbəkələr üçün müxtəlif

tətbiqetmələr yaradacayıq. Bundan sonra proyektiv sahəni təkmilləşdirməklə əlaqəli hakim çoxluqlara və virtual onurğa əsaslı açar köçürmə və dəyişmə adlanan müasir model təklif olunacaq. Nəticələr göstərir ki, kombinator və əlaqəli hakim çoxluqlarəsaslı virtual onurğalı yanaşmalar Kabelsiz Sensor Şəbəkələrdə modelin sensor çevikliyi, resusr effektivliyi vərabitəsi üçün daha yaxşı səmərəlilik və çeviklik dərəcəsi yaradır.

LIST OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Nomenclature

Wireless Sensor Networks – WSNs

Local Area Network – LAN

Digital Signal Processors – DSP

Field-programmable Gate Array – FPGA

Application-specific Integrated Circuit – ASIC

Random Access Memory – RAM

Secure Digital – SD card

Radio Frequency Identification – RFID

Radio Frequency – RF

Industrial, Scientific and Medical – ISM

Electromagnetic Interference – EMI

Analog to Digital Converter - ADC

Multi-point Control Unit – MCU

Global Positioning System – GPS

Condition Based Maintenance – CBM

Balanced Incomplete Block Design – BIBD

Virtual Backbone – VB

Generalized Quadrangles – GQ

Key copying and exchanging – KCAE

Dominators Group – DG

Independent Set – IS

Maximal Independent Set – MIS

CHAPTER 1.

1.1. Introduction

In the 19th century the term wireless communication which will lead innovations in the future was introduced and the technology of wireless communication has developed over the subsequent years. Wireless communication technology is based upon exchanging data or power among points that are not connected by any electrical conductor which uses wireless media such as radio frequency technology to transmit and receive data over the air, minimizing the need for wired connections. Distance between objects may be short, such as a few meters for televisionor as far as millions of kilometers for deep-space radio communications. For instance, cell phones, GPS systems, wireless mice and keyboards, remote controls, wireless routers and wireless devices which can carry information [1].

1.1.1. How does Wireless communication work?

In order to make the most effective use of wireless networking technology, it's still important to understand what's going on inside it.

Initially Wireless communication were intended to sending audio signal through air. Then that signals were called radio and TV appeared when pictures were added to the signals.At the middle of 20th century the word "Wireless" were used less, but at the past two decades it makes comeback owning to Internet.Wireless Internet has made the Internet more convenient than ever before. But what is the difference between Wireless Internet and ordinary Internet access?

It is known from physics changing magnetic field will produce an electric field, and changing electric field will produce a magnetic field. During the time of making regular (AC) current irregular passing from the conductors such as cable, there will be the energy losses due to naturally created field of magnet which will be nearby of the wire. The created electric field by the power of magnet force in the area creates one more electrical field which by consequence is leading of creation another magnet field. This harmony is continuing until the power of the initial current is not enough

and been reduced significantly.Such energy conversion between electricity and magnetic energy is called electromagnetic radiation, or radio waves [2].

Figure 1.1. Transmitter receiver

Electromagnetic energy spreading through space is known as radio. Transmitter is tools which is able to generate radio waves. This device converts electrical signals to the electromagnetic waves that are oscillating. The converted into waves signals rocket in the air with the light velocity. There is an opposite device which is known as receiver. The main purpose of the device is to being able of detection of waves of radios, which have been spread into the air from transmitters. After detecting the waves from the air another main role of the receiver device is to changing them to the different type of energy. As it is shown in the Figure 1.1. both of the devices have been provided with distinct tools which is called antennas. The purpose of having this stick shaped metal parts on the devices is to be able to create streamline for the radio signals. That is to say by creating any pattern or direction effectiveness of the radiation is significantly increased in transmitters and sensitiveness in the receivers [2].

1.2. Wireless network modes

Nowadays Wireless Internet is the simply way to sending and receiving network data by using radio waves. However, low-power transmitters have the negative side

such as sending signals relatively small space. Wireless network may be either the Ad-Hoc or Infrastructure mode of making device connections [2].

1.2.1. Wireless Infrastructure mode

Typically,wireless network uses infrastructure mode. In such mode various devices communicate network through a router or central access point (Figure 1.2).A wireless router is A networking device which forwards data packets in network is called router and also may include the functions of a wireless access point. Usually modem is used instead of router. Low-power radio transmitters and receivers are parts of the modems. Significantly being effected by the material of the walls and electrical devices in the vicinity of modem it is radio signals capacity is between 90 meters or 300ft[2].

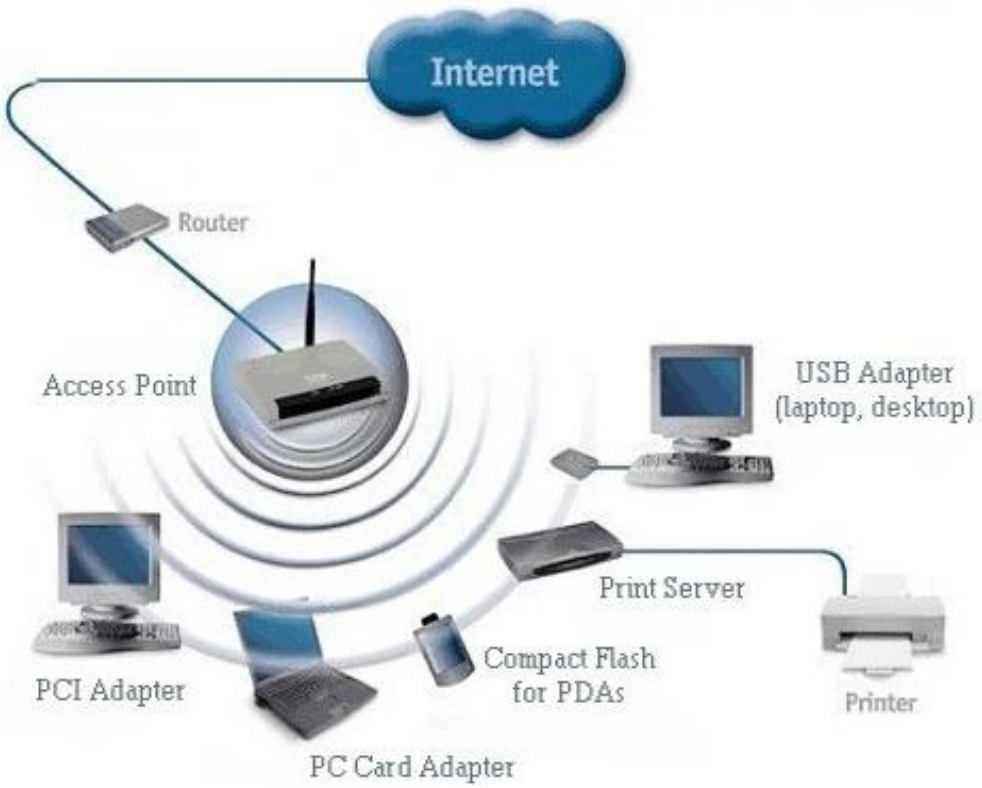


Figure 1.2. Infrastructure mode

1.2.2.Wireless Ad hoc mode

Wireless ad hoc network in other words is called wireless infrastructure wireless mode. As it is depicted in the figure 1.3, unlikely to the infrastructure mode in the wireless ad hoc mode the electronic devices are not central devices vise-versa they are inter connected with each other. As it is known rotors are the devise which were used in order to have connections among the devices through it, however, by the help of using AD hoc networking it is now possible to eliminate that step. That is to say this mode does not require any central device for linking electronic gadgets among themselves.Mean of Ad-hoc network comes from the Latin *ad hoc* which meaning "for this purpose". Ad hoc network contains devices, which are called sensor node, and they are inter communicated among themselves by providing data transportations [2] [3].

An ad-hoc network is a local area network (LAN). It requires minimal configuration and its deployment takes fewer time. This network is capable of to bring into one area various electronic-devices, generally not big devices, so they could be interconnected with each other. The main disadvantage of this mode is that there will be considerable decline in the quality of running once the quantity of the connected-devices will increase. Simply, the main problem will occur that managing of the system will suffer [2] [3].

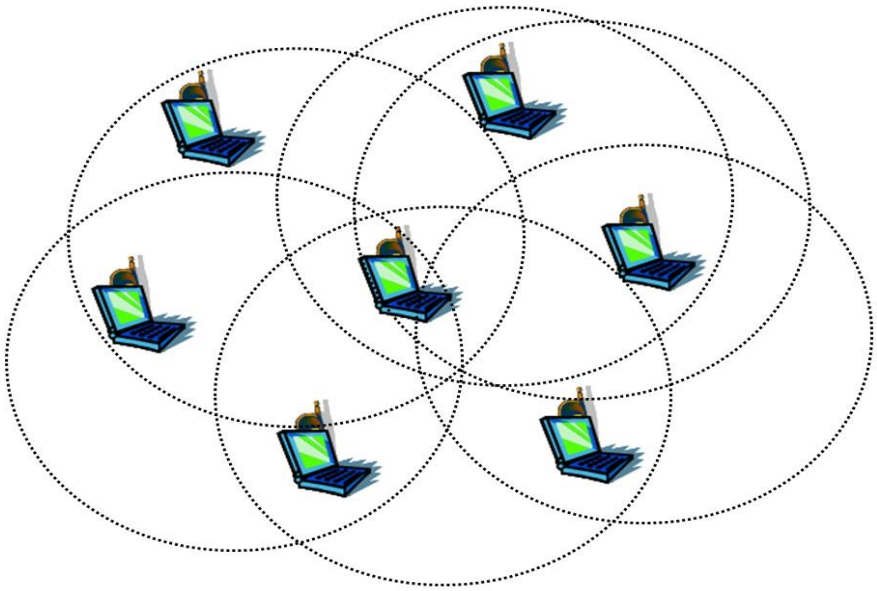


Figure 1.3. Ad hoc mode

1.2.3Characteristics of the Ad hoc network:

Mobility:

The belief in changing the location of modes are the reason of being (raison d'etre) for chaotic/random networks [3].

It is possible of having quickly positioning in one area with the absence of any infrastructure. Having this kind of patterns leads to the procedure that the users now have to discover a location among already created teams or swarms, which are inter-coordinated in order to create missions and tasks [3].

There are numbers of types of mobility such as, group mobility, motion mobility, preplanned routes, random mobility and so on. The causes of the impact on the performance can cause by route scheme assortment which is also highly depending on model of the mobility [3].

Multi-hopping:

Sometimes it is possible to have a not direct way/road from source to a final point thus, this kind of movement is traversing additional nodes. All this kind of dressage are possible to detect by the help of multi-hopping network [3].

The nets which are set accidentally/randomly frequently produce various hops in order to be able to compromise with the difficulties such as spectrum reuse and conversation [3].

There is an operation that is called battlefield cover up (covert) which reduces hops in order to have a decline in the scale of spotting by the fiends [3].

Self-organization:

The network ad-hoc have to be able to independently choose its parameter for configuration. The parameters are being able to address, to route, to cluster, to position an identification and to have a control of power and so on [3].

Often enough, some unusual nodes for instance mobile backbone nodes are able to have motion coordination of themselves and dynamic distribution between the geographic location and source coverage of inaccessible islands [3].

Energy Conversation:

The great proportion of the ad hoc nodes such as, laptops, PDA-s, sensors and son on. are limited by the source of power in order to be able to create their power for themselves likewise, solar systems [3].

It is vital to have a protocol design with a huge productivity, for example MAC, routing, discovery of resource and so on. The mentioned factors increase the life of the assignments [3].

Scalability:

Sometimes random networks have more than 1000 nodes. Generally, it happens when environmental sensor fabric is big enough, in deployments of battlefields, in vehicle grids and so on. The hierarchy in construction of scalability have been played a major role in infrastructure for wireless networks [3].

Before to form an ad-hoc wireless network, it is necessary to configure each wireless adapter for ad-hoc mode instead of infrastructure mode. Besides, it is a well known fact that the adapters which do not have any wire in the network system namely ad-hoc have to utilize identic Service Set Identifier, in other words SSID and their radio channels numbers have to be the same. It is impossible to incorporate Wireless ad-hoc networks to wired LANs or to the internet without installing a special-purpose network gateway [3].

The economic aspect has a big impact on the ad-hoc system popularity and usefulness as if it is required to build a marginal LAN without any wire connections then the cost of the devices for the project have to be optimal, not expensive. This network system also possible to apply like a fallback mechanism, however, not permanently. This mechanism will work in the cases when devices of infrastructure of mode network for instance router or access points stop working [3].

1.3. An overview on Wireless Sensor Network

It has undeniably predicted that for our century one of the mostly used technology will be Wireless Sensor [4]. In the WSN the letters are standing for

Wireless Sensor Networks, respectively. The definition of it means the networks without any wire connections which is self-configured and does not contains any infrastructure. The purpose, aim of these kinds of networks are to provide a monitoring for the ecological or physical conditions for instance heat of the weather, noises, vibration, gravity, motions or toxins and accommodatingly share this gathered information between the network and base locations or sometimes choose/analyze where the information can be monitored and examined[5].

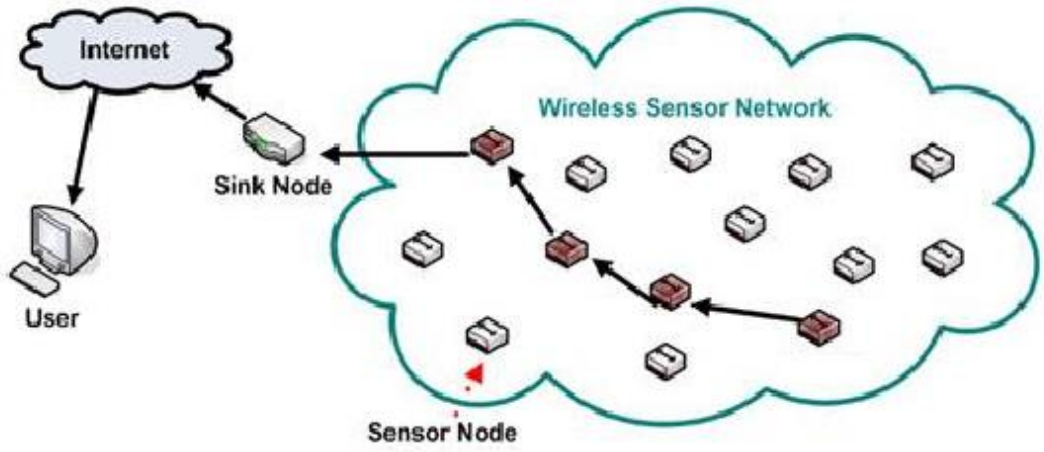


Figure 1.4. Wireless Sensor Network

Generally, more than hundreds of thousands of sensor nodes are exists in the wireless sensor networks. It is known that it is possible to have interconnection by utilizing radio signals among sensor nodes [5].

Sensor nodes in overall have to be able to deliver some simply functions which are listed below in order empower applications that based on WSN.

- Gaining of data and conditioning of signal in/for various sensors
- Ability of data Storage
- Being capable of processing data
- Due to generating alert examining of data after being processed
- Actuation
- Tasks of measurements' Arranging and execution

- Node configuration Controllingand managing
- Ability of forward and transmit as well as receive data packets
- Network and communicating tasks' Schedule and execution[6].

1.3.1. The Network Topology

It is well known that not only a single design exists for the WSNs network structures. There numerous selections for the developer in the stage of designing the network. For example, choosing the topology type is only one of them. There are various several topology types and some of them are listed below [7]:

1) **Single-hop star:**The most of less complicated WSN topology is single-hop star. Straight communication between the gateway and each node has been provided in this kind of topology. Once it is possible by the help of single-hop star topology the problems related with networking is declined significantly, thus by doing so the design is becoming after less complicated. Unluckily, this topology contains some restrictions such as low quality of scalability and properties of robustness. That is to say, it will be observed that once the areas are large enough then the nodes which are the most far was from the gateways will poorly link to them [7].

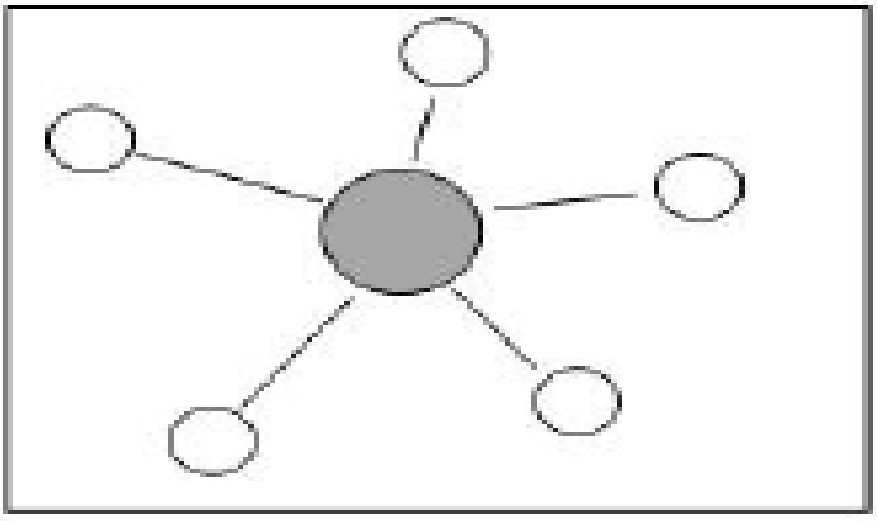


Figure 1.5. Single-hop star

2) **Multi-hop mesh and grid:**Multi-hop routing is required in order to have access bigger locations and networks. Unlikely, from a single-hop star this type of

topology has sensors which passes signals among themselves up to the time when they are in the gateway. A special protocol of routing is capable of finding the route of the signal, we will come back to this topic and discuss it thoroughly in the chapter 3. In the two figures below it has been depicted the differences when the structure of WSN is configured, see figure 1.6 on the right side or organized by randomly, see figure 1.6 left side [7].

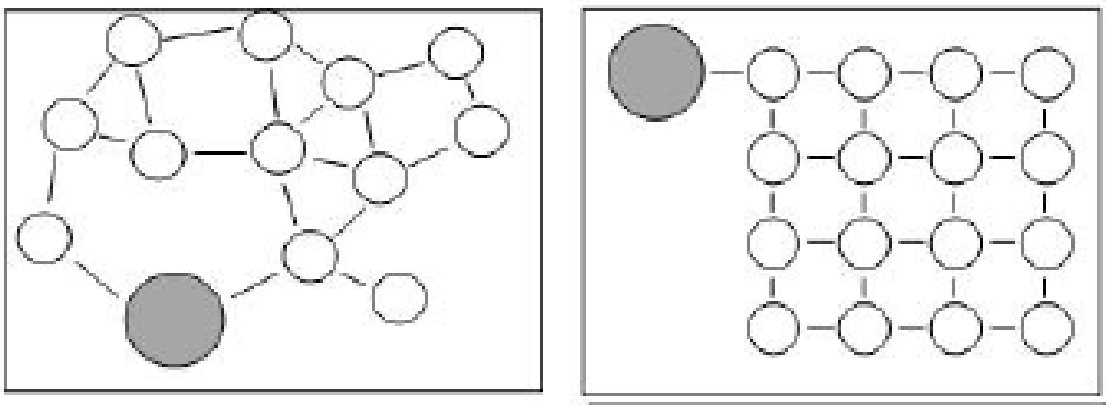


Figure 1.6. Multi-hop mesh and grid

3) **Two-tier hierarchical cluster**: Two-tier hierarchical cluster architecture is one of those architectures, which is mostly used when WSNs are large. Cluster head is a location where all data has been sent from the nodes in the special region, in these type of topologies. The cluster heads are interconnected in different regions by creating a network. It is possible that this network will increase its dimensions by sharing clusters data. That is to say cluster heads will send data which they have into new cluster heads and so this pattern will continue until reaching the gateway. Once the large structure which was built by hierarchy is divided into numerous zones it became possible to route and perform locally in these areas. If it is required to have more reliable and high transmission speed it is possible to utilize wires for cluster heads. It is possible to change a design of cluster heads in order to make them better in tasks for computation and communication [7].

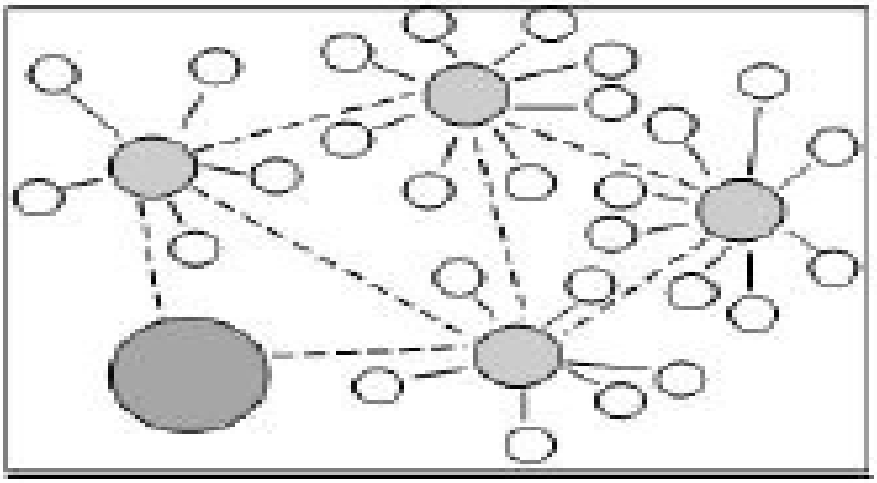


Figure 1.7. Two-tier hierarchical cluster

1.3.2.Sensor Node Hardware

All sensor nodes consist of four typical sub-systems, which are;a computing sub-system, a communication sub-system, a power sub-system, a sensing sub-system [7] [8].

1) **Computing Sub-System.**

If any computations areneeded, then computing sub-systems is required. These systems are also take care of some other task such as to control the components of sensor nodes. The process unit and storage unit are two parts of the sub-units. Unlikely of others, here processors have various mode for operating and it is generally Active, modes of Idle and Sleep is as low as possible, it is vital characteristics in processors which are in sensor nodes. The advantage of having this is can be monitored when it is saving power independently, without obstructing the processor's operation once it is necessary [7] [8] [9].

There are other components inside the sensor nodes those functionalities are controlled by controllers. Controllers also do some tasks and examine data. The most popular among the controllers is microcontroller. There are other types of controllers, some of them listed below [8] [9]:

- desktop microprocessor (for general use)
- digital signal processors

- FPGAs and ASICs

Due to the fact that, microcontrollers are not expensive and they cost a reasonable amount of money plus it is very easy to have a link with other devices moreover they do not require a lot of power to work and not complicated to program them it is shown that they have been frequently utilized in the sensor nodes which are one of the embedded systems. Microcontrollers' power consumption is lower that power consumption for microprocessors. Thus, that is the reason why in a sensor node it is better not to have it. Digital Signal Processors (DSP) sometimes used as broadband in applications for communication, which have not any wire connections. However, the most modern wireless communication belongs to Wireless Sensor Networks. Hence, its benefits are such as, being less complicated and process of signal analyzing for sensors in data are simpler. Hence, the positive sides of DSPs generally, does not play a big role for sensor nodes which are wireless. Depending on the what has been required it is possible to program and configure again field-programmable gate array (FPGAs), however, time and man force consumption of this task is more that it is anticipated [8] [9].

There are mainly two components in the storage nodes namely:

- Flash memory
- RAM

The duties of the RAM are to store computations data and information which is sensitive. Whereas, flash memory has got only code of the program for the node [7] [8].

In order to be able to retrieve via capturing off-line data after while certain motes contain non-volatile storages. Shimmer mote for instance created Secure Digital (SD) card that will be able to keep storage almost two gigabytes. Though, it has pros as well as cons. Hence, the downsides of it is that these kind of selections are available only when power deliveries are big enough. Various sensor nodes can have various capability for storage, for example, it can even be magnitude order and more. Accordingly, what has been wanted the selection take place against the additional finance which will be required for this actions [7] [8] [9].

2) **Communication Sub-System.**

For providing a communication among the sensor nodes and base station communication sub-system is created. Usually, short range radios have been used as a communication sub-systems, however, depending on the demand inductive fields as well as ultrasound fields utilized too [8] [9].

Although the infrared communication is possible to use with small power supply and it is comparatively not expensive, as a negative side it requires line of sight among the interconnected devices which is unobstructed.As network coordinator demands high power consumption it bring to the failure of ultrasound. Besides, another problem such as miniaturization which is form factor for the equipment is a vital problem, as well. Although communication of inductive fields is applied widely in Radio Frequency Identification (RFID) applications it is not applicable due to the fact that it demands high power supply for the coordinating network and additionally it has got very short range [7] [8] [9].

As Radio frequency (RF) communication does not restricted by line of sight and it is possible by the help of modern devices to implement low power radio transceivers which are provided in date rates and accordingly scalable ranges for application this communication is the best for sensor nodes. A great amount of the governments have regulated the Radio frequency (RF) spectrum as it is an uncommon, rare resource. Some bands such as, Industrial bands, Scientific bands and Medical (ISM) bands are appearing to be as unlicensed bands thus, it means if the device follows the band control rules then this is unchangeable to operate it. Initially, ISM bands are designed in a way that it was permitted electromagnetic interference (EMI) emissions from the products without interfering with other devices so not causing any difficulties to them to be drained in. The devices even those which, does not have RF communication can be taken as a possible basis for interference. Moreover, 900-1000MHz is the range of resonations which humans feel hence, individuals are influenced by the effects of the communications via ISM bands and our frequencies multiplication. Nevertheless, because of the reason of reducing the charges on this wireless sensor networks (WSNs) try to be internally operated parts

of these bands. Devices which deliver an extra interference such as wireless local area networks, wireless keyboards, home automation systems, wireless surveillance cameras and so on. which are operate in the bands those are unlicensed and the fact that they are in various versions from region to region is the issues which have to considered [7] [8] [9].

A various range of radios have been utilized for sensor nodes. The radio chip which confirmed by IEEE 8-2.15.4 standard was recently use, however, there are alternatives such as Bluetooth, as well. The main advantage sides of utilizing Bluetooth are those it will be a way easier to be connected with the devices such as laptops and mobile phones without adding to them any electronic parts. The drawback of using this method is the requirement for additional power supply. Previous groups of nodes used the radios those were not a part of any standards at all or only belonged to proprietary standards [8] [9].

3) **Power Sub-System.**

Usually, a battery is the part of power sub-system and provides energy supply for the sensor nodes. There could be various applications in wireless sensor networks which can prolong for weeks, months and sometimes years hence, in this kind of cases it is very hard to change batteries especially, when there multi-thousand nodes and located in dangerous places. Due to the mentioned above facts the developers have to be sure that every feature of the WSN is as much as efficient as possible. Thus, communication and localization algorithms, sensing electronic devices and so on. should be chosen in way that their energy consumption is as minimum as possible [8] [9].

Sometimes, in order to charge again the battery in the site power generators are utilized. Accordingly, on the place of the nodes the power supply sources can be different such as, photovoltaic, thermoelectric and motion or vibration energy conversions [7].

Actually, when applications od sub-set of WSN is large enough then energy consumption is the main limiting issue. Apart from being used in significantly widespread of deployments wireless sensor networks (WSNs) they are enable to be

used in ordinary cases, as well. For instance, in the industrial monitoring, sometimes wired network infrastructure, wireless local area network infrastructure does not exist in the plant hence, it is very expensive to add, however, frequently in the place the power infrastructure is installed already. By having permission to change the batteries or charge them time to time the sensor nodes exist in multiple health applications. There are even more complicated as well as interesting research issues about the fact that primary capacity of energy which generally was ignored. The mentioned category, however, has got sensor networks which are commercially feasible for now. Right now the only accessiblesolutions for the main problems for example, data aggregation and querying and so on. those impact these kinds of networks are sub-optimal solutions [7] [8] [9].

4) **Sensing Sub-System.**

The devices which makes electrical signals by translation from physical phenomena are called transducers. Thus, the connection to the world of the nodes are sensing sub-systems. Analog or digital signals can be types for output signal for the sensors. For being able to be read by the processors the nodes must have an analog to digital converter (ADC) for the data once the output is analog. Sometimes, some sensors for example, temperature, humidity and light are installed in the nodes on the Tmote Sky as well as 3 accelerometers to the Shimmer, however, some of them do not have. The nodes those do not have this kinds of installed sensors are arranged with appropriate ports which give permission to different sensors to be connected so to have better versatility [7] [8] [9].

Attaching Analog sensors are complicated, however, usually this action, attaching to the mote is very simple for sensors which have digital output. ADC should have a node, however, if it does not exist then have to be built. Frequently MCU receives numerous interruptions from external ADC(s) if they do not have a proper design. As a results of those interruptionsthe additional functions of the nodes are negatively affected. Nowadays, Atmel ATmega 128 L as well as Texas Instruments MSP430 processors for the sensor nodes are the most popular and they have provided with integrated ADCs. Numerous applications are not find good

enough the quality as well as resolution which ADCs have got. ATmega 128L provides only 10bit ADC whereas, MSP430 suggests 12bit ADC [7] [8] [9].

Moreover, Global Positioning System (GPS) too which is detecting the locations unit can be added to the sensor nodes or mobilizer and so on. Numerous conditions for instance temperature, humidity, pressure which are ambient, objects' characteristics and motion of theirs are monitored by the help of various kinds of sensors for example, seismic, thermal, visual as well as infrared. In the figure 1.8 the main overview and some basic but vital components are depicted whereas, figure 1.9 describes typical and common sensor node [7] [8] [9].

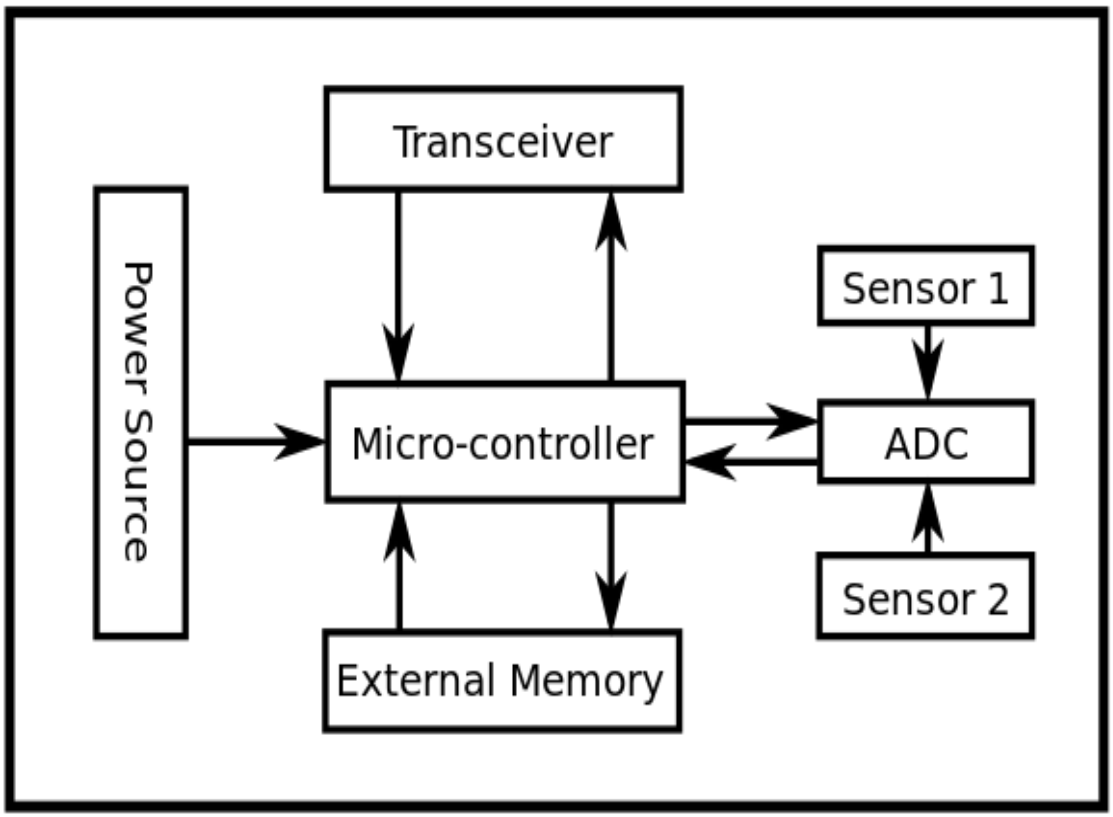


Figure 1.8 Basic overview of important components

Figure 1.9Typical senor node

1.3.3. Sensor Node Software

Normally, there are 5 sub-systems which are common sensor node's applications of software. They are listed below [7]:

1) Operating System Microcode.

Operating System Microcode is mentioned like middleware too. In order being able supporting a numerous function by software modules which are described as a high level and that software utilize the represented code. The machine level functionality software for the microprocessor is covered by middleware too. For instance, the most popular common use is TinyOS which is sensor networks' operating system [7].

2) Sensor Drivers

The software modules which, able to control simple functions in the sensor transceivers are sensor drivers.Accordingly, with the kind of the sensor, they are able to upload the correct settings as well as configuration into it [7].

3) Communication Processors

Routing, packet buffering are communication functions as well these functions are controlled by communication processors. Also forwarding, topology maintenance and medium access control for instance connection mechanisms, direct sequence spread spectrum mechanisms so on. as well as encryption are controlled by communication processors [7].

4) Communication Drivers

Details of the Transmission connections of the radio channel such as clocking and synchronization, signal encoding, bit recovery and bit counting, signal levels as well as modulation are operated by these software modules [7]

5) Data-Processing Mini-Applications

It includes simple applications such as processing of data, storage and the manipulations of a signal value and so on. In order to achieve a processing in thein-network these are have a support in the level of node [7].

1.3.4. WSN Routing

One of the many vital tasks in WSN is routing thus need to be carefully controlled. In order to have data transportation among the sensor nodes and the base stations the techniques of routing are utilized, thus communication is achieved. There are multiple routing protocols accordingly with the applications.The main issue on the routing isto optimize the lifetime of the network so reduce it meanwhile not having an increase in the power supply for it. Hence, numerous protocols of routing were established for the purpose of reducing consumption of power while increasing the lifetime of the network. There are categories for the routing protocols which are defined accordingly with the participation of the nodes, clustering protocols, functioning mode and structure of the network. There are multiple difficulties in the routing such as, consumption of the power, deployment of the nodes, scalability, connectivity, coverage and security[10, 11].

Accordingly, with the structure of the network usually, routings on the WSNs are possible distributed as flat based routing, hierarchical based routing as well as

location based routing. When all of the nodes have the same responsibilities or functionalities then this type of routing is flat based routing. Whereas, nodes are doing various responsibilities of the network in the routing which based hierarchically. Meanwhile, locations of the sensor nodes were exploited to the route data which is in the network, this is for the location based routing. Some parameters of the system when are under control then a routing protocol is assumed as adaptive in the purpose of getting used currently available network conditions and accessible power levels. Moreover, there some classifications for the mentioned protocols such as, multipath based, query based, negation based, QoS based and sometimes it is coherent based routing techniques accordingly to the operations of the protocol. Furthermore, there are three classified categories for routing protocols such as, proactive, reactive as well as hybrid changing accordingly the way of searching for the destination of the route. Before there is a demand for the routes all of them have been computed in the proactive protocols whereas, only after there is a need for the routes they are computed in the reactive protocols. When the mentioned two actions are mixed, or combined then it is called Hybrid protocols. Table driven routing protocols are those protocols which were used when sensor nodes are not moving rather utilizing reactive protocols. There is a huge amount of power supply for discovery of route as well as for reactive protocols. Cooperative routing protocols are other types of protocols where, central node receives data from other nodes. In the central node, the received data is possible to be combined and can be processed after, however, route cost reduction will lead to power use. Locating and timing of the data is relied by the significant amount of various protocols. Classification is utilized accordingly with the network structure as well as operation of protocol or routing criteria in the purpose of streamline the survey[10, 11].

1.3.5. WSN security [12]

1. WSN security obstacles. In contrast with the traditional networks WSN is a distinct network and has got numerous limitations. Implementation directly is hard in current mechanism of security in the WSNs is very complicated because of the

limitations. Thus, when creating a useable security mechanism by taking the ideas from the nowadays' security techniques it is demanded to verify these limitations before [12]:

- Very Limited Resources

Some volume of resources is demanded by all security approaches in order being able to implement, include data memory, code space as well as powering energy for the node. Nevertheless, nowadays the mentioned resources are restricted in a small wireless sensor [12].

• A small amount of memory as well as storage space for the code is called Limited Memory and Storage Space. The code size in the security algorithm has to be restricted for being able to have security mechanism which is effective [12].

• For having capability in the wireless sensors restrictions in the power supply, thus Power Limitation energy is the main limitation. When sensor network field received sensor nodes and they are deployed there it is impossible to charge them again or replace. That is the reason why, in order prolonging the life of the particular sensor node its battery have to be reserved. During implementation of a cryptographic function or protocol inside the sensor node, if security code has been added into a sensor node, the its affect into the security code must be taken into account [12].

- Unreliable Communication

Another danger for the sensor security is unreliable communication. Defined protocol is the mainly reliable source for the security of the network, thus it is depended to the communication, as well [12].

• Unreliable Transfer. Usually, since the packet-based type of the routing in the sensor network does not have connections so it is inherently unreliable.It may be resulted to lost or missing packets in the channel errors damaged or get dropped items from the height into the congested nodes [12].

- Unattended Operation

Accordingly, with the function for the individual WSN, it is possible to left sensor nodes unattended for extended duration of time. Mainly unattended sensor nodes are divided into three caveats mentioned below [12]:

• Exposure to Physical Attacks:It is possible that the sensor will be affected by environmentopen to adversaries such as bad weather, and so on [12].

• Managed Remotely: It is possible for physical tampering such as through tamperproof and physical maintenance like replacing of batteries problems to be virtually undetectable by the help of Remote management of a sensor network [12].

• No Central Management Point:Central management point should not exist in the distributed network which is a sensor network too. By having so, the importance of the sensor network will be increased, however, the design should be faultless if not then difficulties will reduce efficiency of the network and create additional issues [12].

2.Security Requirements. One of the unique kind of the networks is WSN and thatis the reason why it requires some sort of special demands. Thus, there are unique demands as well as simple networks demands for WSNs [12].

- Data Confidentiality

The first issue which any network will face is the confidentiality of the data. The below mentioned are the factors which related with confidentiality in WSNs [12].

• There should not be any sharing among the sensor networks' neighborhoods, specifically, if it is in the army system, so the data at the storage can be very important and sensitive [12].

• It is very common for applications that in them the nodes will have access to the very important data such as key distribution, thus, a secure channel has been created for that in the WSN [12].

• In order to have a protection from the traffic analysis attacks public sensor information for instance, sensor identities as well as public keys, should have to be encrypted too [12].

The encryption of the data is a very typical and simple procedure for protecting an important data with a special key that will be known only receivers so by doing so the confidentiality will be achieved [12].

- Data Integrity

Having confidentiality will prevent the adversary to steal the data. Nevertheless, the information still is not fully safe [12].

- Data Freshness

The freshness for the all of the messages have to be achieved even when they have confidentiality as well as integrity. The reason beyond that is by doing so it is possible to identify if the data is new or old so fresh or not which means the old messages have not been replayed [12].

- Availability

It will cost to have a traditional encryptions' algorithms which will be suitable for WSN. Sometimes it is possible to use again the code by modifying it. Moreover, sometimes it is known that by using additional communication it is possible to reach the same goals. Additionally, sometimes by simplifying the algorithm it is possible to have some restrictions on the data access. All of the above mentioned ways have drawbacks due to the reasons which are mentioned below [12]:

• When it is required to compute more the additional energy supply is required.In the case of not additional power supply the existed data will disappear [12].

• When it is required to communicate more the additional energy supply is required, as well [12].

• In the case of utilizing central point scheme a single point failure is depicted which is a major threat for the network availability. Having the security is very important for network operations as well as keeping accessibility for the whole network [12].

- Self-Organization

Depending on the various conditions each sensor nodes have to be able to organize itself and heal itself independently as well as flexible are the main

requirements in the typical WSN ad hoc network. Fixed infrastructure for the before mentioned sensor network management does not exist, hence, it creates an additional challenge for the security of the WSN [12].

- Time Synchronization

Time synchronization is reliable for many applications in sensor network. Particular radio of the sensors can be turned off for some time so the power saving is achieved [12].

- Secure Localization

Frequently, correct and automatic location of the sensors in the network ability helps utility sensor network. The correct info about the location is required by the sensor network which is built to find faults. Thus, having so pinpointing the place of the fault will be possible. Unluckily, the attacker can report wrong signal strengths, reply signals and so on. in order to simply manipulate info about the location [12].

3. Attacks. Likewise, other networks WSNs been faced attacks by numerous sources. It is not doubtful that the quality and difficulty of the attacks are having an increasing trend. There are numerous ways of conducting these attacks. One of the most popular one is DoS attacks as well as via traffic analysis, privacy violation, physical attacks etc. [12].

- Types of DoS attacks

A typical attack for WSN is jamming one node or a set of nodes. The term of jam in this scenario stands for the action of transmission radio signal with its frequencies which is utilized by WSN. There are two types of jamming a network: Constant jamming and intermittent jamming [12].

It is possible to have attack itself in the link layer made. One of the option can be that the attacker is basically deliberately violating the communicating protocol as well as continuously transmitting messages in order to try creating of collisions. It is required to transmit again the packet which affected from these collisions. By the help of utilization of this method the attackers may easily drain the energy from the power source via repeating the same transmissions [12].

By easily rejecting of routing messages a node will have an advantage in multi-hop network at the layer of route. It is possible to do this process continuously and irregularly depending on the net results which shows that it is impossible to share or receive any messages into network or into part of the network via neighbors' which routes from malicious nodes. As transport layer is very vulnerable it is possible to be attacked, for instance via the flooding case. In this flooding method the considerable amount of connection requests has been sent into the vulnerable node. Having so, the resources have to be able to manage all of the received requests for connection [12].

- The Sybil attack

The malicious device which not legitimately takes numerous identities is described as Sybil attack. Initially, it was known like the attack which was able to win the redundancy mechanisms in distributed storage data systems at peer to peer networks. Moreover, for defeating the distributed storage systems a Sybil attack is very good also in terms of routing algorithms, data aggregation, voting, fair resource locations as well as foiling wrong behavior detection [12].

- Traffic Analysis Attacks at WSN

Generally, the communication exists between the composed many less power sensors and in comparison robust and high power base stations. Thus, it is very common for the data to be collected in one nodes which is at the end is routed to the base station. Frequently, the attackers are able to totally disable the whole base station, thus effective rending the network adversary does not help [12].

If we research the rate of the attacks, then it is possible to have a conclusion that the nodes which have a location closer to the base stations are forwarding more packets in comparison with the nodes which have longer distance from the base stations. The main role of the attacker is monitoring the packet sending nodes and following the nodes those who send greatest packets. While, in correlation attacks the adversary just creates events as well as monitoring of nodes which sends its packets [12].

- Node Replication Attacks

Theoretically, it is not complicated at all to understand the replication attack of a node. The process if depicted like the attacker's main aim is adding a node to the WSN which already exists so it does by replication of the ID of the sensor node which already presented and currently available. A replication of the nodes might create disruptions of the performance of the sensor networks by corrupting as well as misrouting it. The final results are generally, disconnections from the networks and false reading of sensors [12].

- Physical Attacks

Usually, the operating environments of the sensor networks are outdoor whereas it is very possible to physically attacked as their dimensions are very small. The sensors are permanently destroyed if attacked physically. It is not likewise the other attacks which have been mentioned above so in this attack the damage is not curable [12].

4. Defensive Measures.

Considering the issues related with security for WSN it is suggested three more challenges for having better security at ad hoc networks [13]:

- Key Management in WSN

Privacy, integrity as well as authentication services are vital for prevent the adversary from damaging the security at WSN. In order being able of establishment the key parameters on the system the key management is critically utilized for achieving protection of WSN. Nonetheless, taking into account the nature of the ad hoc the creation of key management is complicated as well as the restrictions of the resource in the network environment is creating even additional challenges [13].

- Securing routing of WSN

It is well achieved to cope with the dynamic topology with the help of the current protocols for routing, however, frequently it will suggest very less or even not at all security precautions. Additional issue on this is implementing the security routing protocol for the network environment together with dynamic topology, vulnerable nodes, restricted computational abilities as well as strict power limits [13].

- Prevention of Denial of service

In reality, nevertheless generally the term Denial-of-service (DoS) isreferring to an attempting of adversary for disruption, subvert and destroy the network, the DoS attack is little bit different. Thus, it is an event whichcontracts or removes the capacity of the network by stopping its predicted performance. There are numerous factors those create the DoS such as, failures of the hardware, software bugs, exhaustion of the resource, environmental conditions or any complex interaction among these issues. The adversary might create a considerable of DoS attack capabilities in WSN. For instance, it is possible to deploy an enemy region of a wireless sensor network. If the enemy already has got the network with the wire as well as power grid and able to have a communication with the lately deployed sensor network, then it is able to create a disruption for the new network[13].

1.3.6. WSN applications

WSN has numerous applications:

1) Process Management:

It is frequently used in the purpose of monitor the area at the WSNs. In this process, a WSN is deployed to the area which time to time shows the phenomenon. A sample from the military data can be utilized the sensor for detecting the enemy intrusions, whereas, more urban examples are could be geologically fencing the oil or gas pipelines. It is undeniable that monitoring the area is one of the vital parts of it [3].

2) Healthcare monitoring:

There are two types of medical applications such as wearable and implanted. The devices which direct contact to the human body or at least they are at the very close distance are called wearable medical devices. The medical devices which are artificially located in the human body are called implantable devices [3].

3) Environmental or/and Earth sensing:

The applications which helps us on monitoring the earth are countless. We will talk about some of them below. The main common fact about them is their ability to

be able to operate in the harsh environments with the requirement of the low power supply [3].

4) Environmental pollution monitoring:

It is now have been applied this technology in the many regions of the Earth such as, London, Stockholm and Brisbane in order to be able to gather the data about the level of the poisoned and dangerous gases in these cities [3].

5) Fire detection (at the Forests):

There are some sensors nodes which are able of detecting the fire at the forests. It is done with the help of the nodes which are provided with special sensors. These sensors are capable of measuring the humidity level, the temperature and the level of each gas during fire [3].

6) Landslide detection:

By the help of the wireless sensors network it is possible now to monitor the small movements of the land layers and predict huge landslides before [3].

7) Monitoring the quality of the Water:

It is very popular to utilize the applications which are provided with wireless sensors to monitor the quality of the water at the various locations such as, lakes, oceans, rivers as well as underground reserves in order to create a proper map of the conditions of the water at these places and be able to control them in time if necessary [3].

8) Natural disaster prevention:

During the natural disasters it is generally said predicting it was not possible, however, nowadays by the help of the wireless sensor networks it is possible. For instance, before the floods Wireless sensor networks are able to monitor and gather information about the changes at the river level in real time with high effectiveness [3].

9) Industrial monitoring:

a. Machine health monitoring: CBM which means condition based maintenance for which the wireless sensor network is created. CBM is providing considerable workers savings and creates additional functions [3].

b. Data logging: It is already mentioned that WSNs are designed for collecting the information for the observations purposes of the environment. The information is generally, such as temperature, humidity and so on. Mainly we need these sensors to be installed at the nuclear power plants too. The most important advantage of wireless sensor networks in comparison with conventional information collectors their ability to send the data real-time [3].

c. Waste water or water monitoring: It is very important to monitor the quality of the water for keeping the humans of the country healthy and the animals of the regions and other habitats which using the water resources healthy [3].

d. Structural Health Monitoring: By the help of the wireless sensor networks it is possible of monitoring the structures of the civil buildings the geophysical processes which are related to them at the rea time.

CHAPTER 2.

Definitions and Preliminaries

Today most of the real life situations can easily be described by the use of various diagrams. One of the most widespread type of diagrams consists of a set of points and a set of lines which connects these points. For instance, in a Google Maps application these points could represent destinations, with lines representing distances between them; or in a family tree the points could represent family members, with lines representing relations between tem; or in a local area network the points might be computers, network devices, with lines representing communication links [14].

In our world everything is linked: cities are linked by roads, railways and flight networks. The different components of an electric circuit or computer chip are connected and the paths of disease outbreaks form a network. Scientists and engineers want to analyze, understand and optimize these networks. And this can be done using graph theory. For example, mathematicians can apply graph theory to road networks, trying to find a way to solve traffic jam problems [14].

2.1 The Origins of Graph Theory

Graph Theory began with Swiss mathematician Leonhard Euler in his study of the ‘Königsberg bridge’ problem. The ‘Königsberg bridge’ problem originated in the city of Königsberg(Germany) lies along the Pregel River. The river has several branches, dividing this city into 4 districts, connected by 7 bridges (Figure 2.1.). People staying there always wondered whether was there any way to walk over all the bridges once and only once[14].

Graph theory is becoming increasingly important as it is applied to many areas of mathematics, science and technology. For example, this theory used for finding the shortest path by GPS, map coloring, ranking hyperlinks on the internet and also finding communities in networks[14].

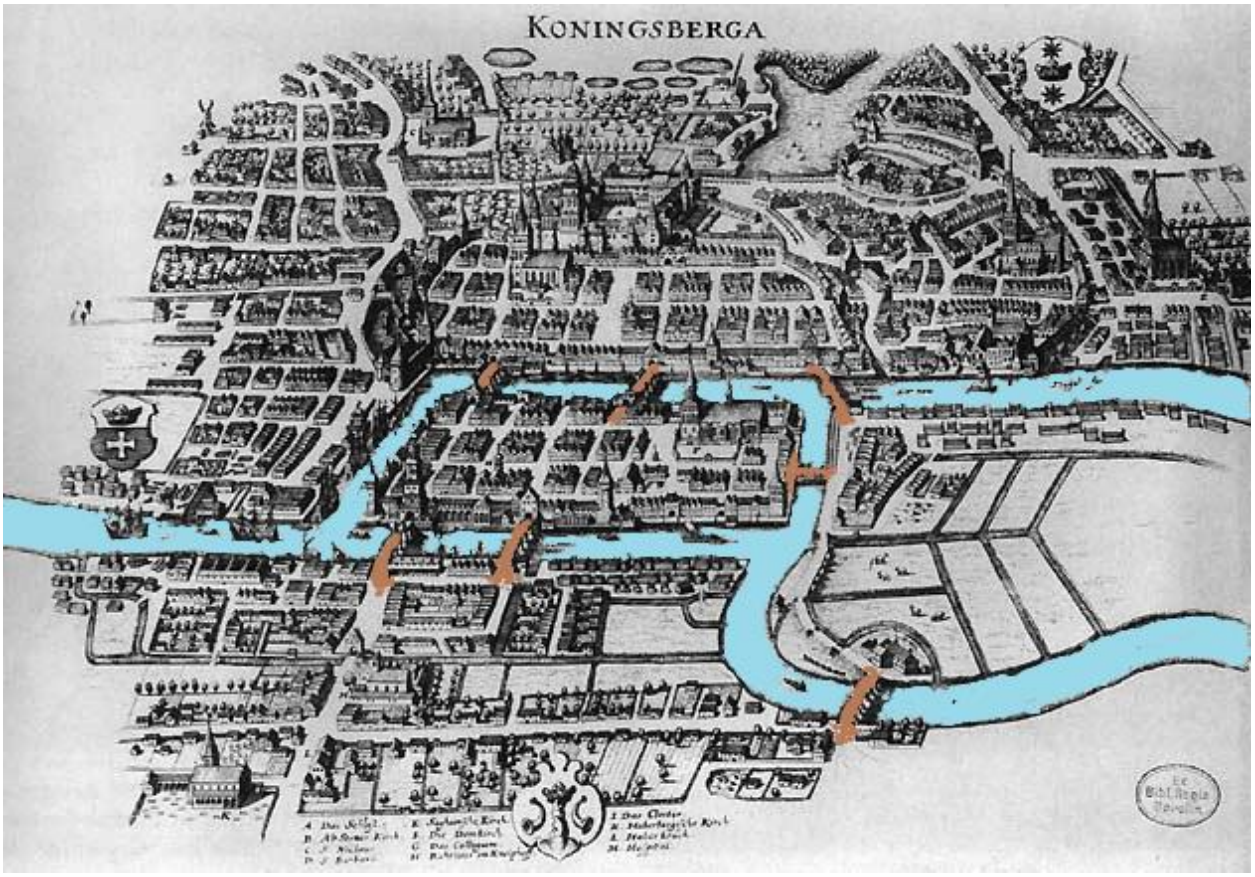


Figure 2.1 Illustration of Konigsberg

In, 1736 using an illustration Leonard Euler proved that it was not possible to walk through the all bridges only one time. In coming to this conclusion, he formulated the problem in terms of graph theory. So he drew a picture that consisted of 4 dots representing four different areas on the map, and connected them with 7 lines. (Figure 2.2)[14].

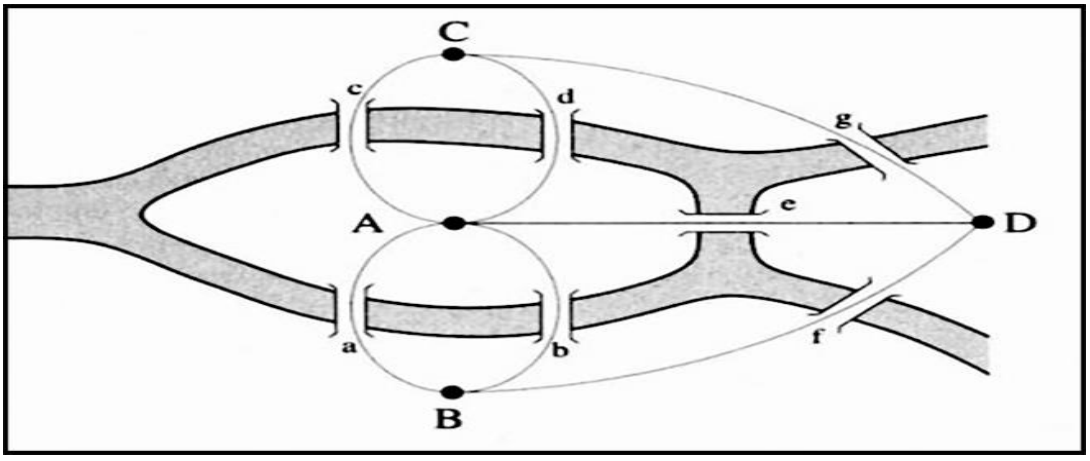


Figure 2.2 Leonard Euler's Approach

By eliminating all unnecessary features this picture consists of dots and lines called as a graph. That graph might have looked somewhat similar to the figure shown below(Figure 2.3.)[14].

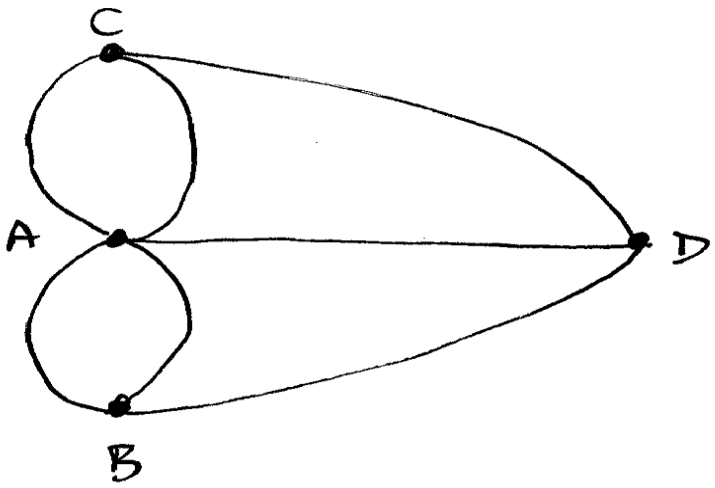


Figure 2.3 Illustration graph of the city

Figure 2.3. simplifies the problem to great extent. Now, the problem can be merely seen as the way of tracing the graph with a pencil without actually picking up it or retracing any segment already drawn[14].

2.2 What is a graph?

A graph is a pair G = (V, E) of sets, where V is the set of vertices and E is the set of edges. Graphs can be represented graphically. Therefore, they are named such. The vertices may be also called nodes or points. Usually a set of V is a finite nonempty set. The edges may be also called lines. The elements of a set E formed by pairs of vertices. That is why for a set of E are adopted $E \subseteq [V^2]$. If vertex set of a graph is V, then it is called graph on V. The vertex set of a graph G is denoted V(G), its edge set as E(G) [15, 16].

There is not generalized correct way to draw any graph. Simply, the dots are noted for each vertex and connecting couple of noted dots by a line if the appropriate couple of vertices form an edge (Figure 2.4.).There is not any specific rule for nodes how to note and for lines how to connect appropriate nodes: nodes may be note as

either a dot or a circle and lines may be drawn as either straight line or curved line [15, 16].

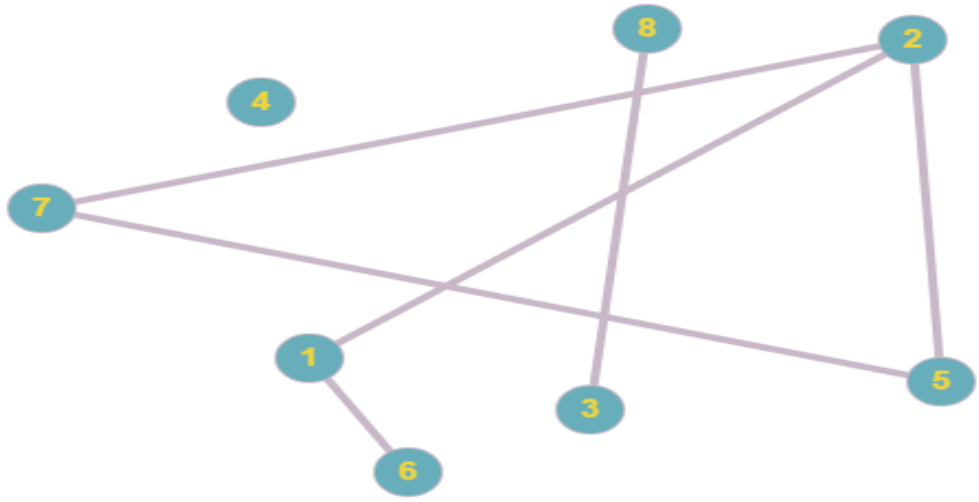


Figure 2.4 The graph on V = { 1,...,8} with edge set E = {{ 1, 2 }, { 1, 6 }, { 2, 5 }, { 2, 7 }, { 3, 8 }, { 5, 7 }}

2.3 Definitions of graph elements

The order of a graph G is number of vertices of a graph and written as |G|; its number of edges is denoted by ||G||. In Figure 4, |G| = 8, ||G|| = 6 [15,16, 17].

Graphs may be either finite or infinite. It is according to their order. If vertex set of a graph and edge set of a graph are finite, then it is finite graph. Otherwise the graph is infinite. The graph is the null graph if it has no vertices and hence no edges. There is also trivial graph which has just one vertex [15,16, 17].

Consider v, u ∈ V(G) and e ∈ E(G). A vertex v is incident with an edge e if v ∈ e. In this case e is an edge at v.Two vertices v and u are adjacent or neighbors if v ∈ e and u ∈ e. So nodes v and u are incident with edge e and meantime u and v are end vertices (ends) of e and e joins u and v [15] [16].

Open neighbor set of a vertex v in G is the set of points that neighbor of v and is denoted by $N_G(v)$, or briefly by N(v). Closed neighbor set of a vertex v in G is the set of neighbors and v itself and is denoted by N[v]. So N[v] = N(V) ∪ {u}. In Figure 2.4, open neighbor set of vertex 2 is N(2) = {1, 5, 7} and closed neighbor set of vertex 2 is N[2] = {1, 2, 5, 7}[17].

Two different edges e ≠ f of a graph are adjacent if they have common end. If each vertices of graph G is adjacent to other nodes of a graph G, then G is complete graph. A complete graph on n vertices is a K^n. A triangle graph is complete graph on 3 vertices (Figure 2.5.) [15,16, 17].

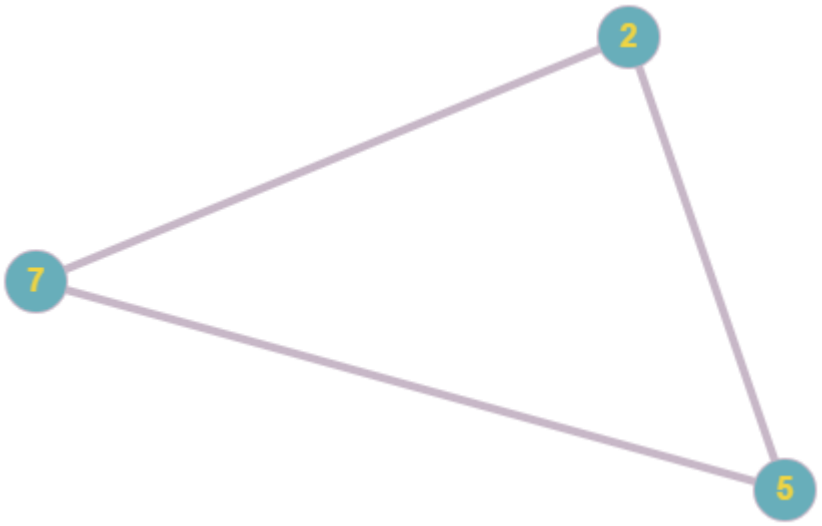


Figure 2.5 Triangle graph

Let's take a look at two graphs: G = (V, E) and G' = (V', E'). A graph G' is termed a subgraph of a graph G if V(G') ⊆ V(G), E(G') ⊆ E(G). In this case, it is reported as G contains G' or that G' is contained in G, and write G ⊇ G' or G' ⊆ G. and a graph G is termed supergraph of a graph G'. A null graph is subgraph of all graphs. Graph in Figure 2.6. is subgraph of graph in Figure 2.4. and graph in Figure 2.4. is super graph of graph in Figure 2.6. [15,16, 17].

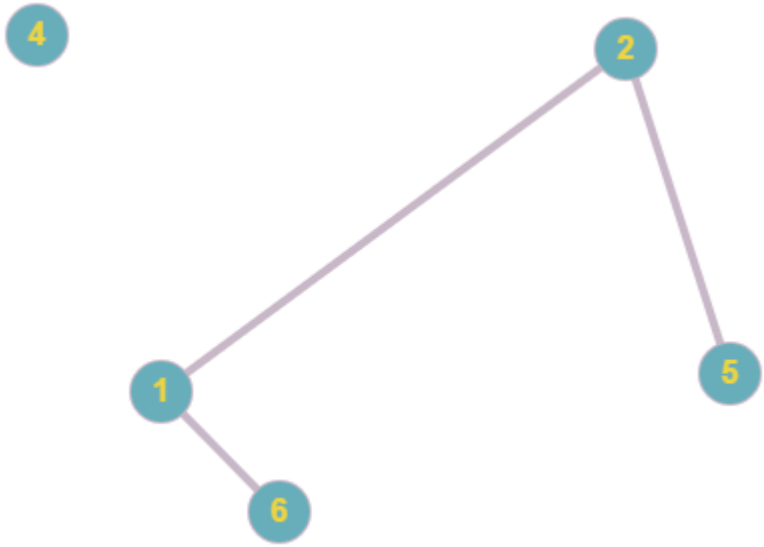


Figure 2.6 Subgraph

When graph theories are applied to practicable problems, sometimes it requires additional aspects correlated with edges. Let there is a value $\omega(e)$ correlated with each edge $e \in V(G)$, called weight.In this case graph G together with additional aspects on its edges, is termed a weighted graph (Figure 2.7.) and denoted by (G, ω). It may be various types parameters as weight: time, distance, value and so on [15,16, 17].

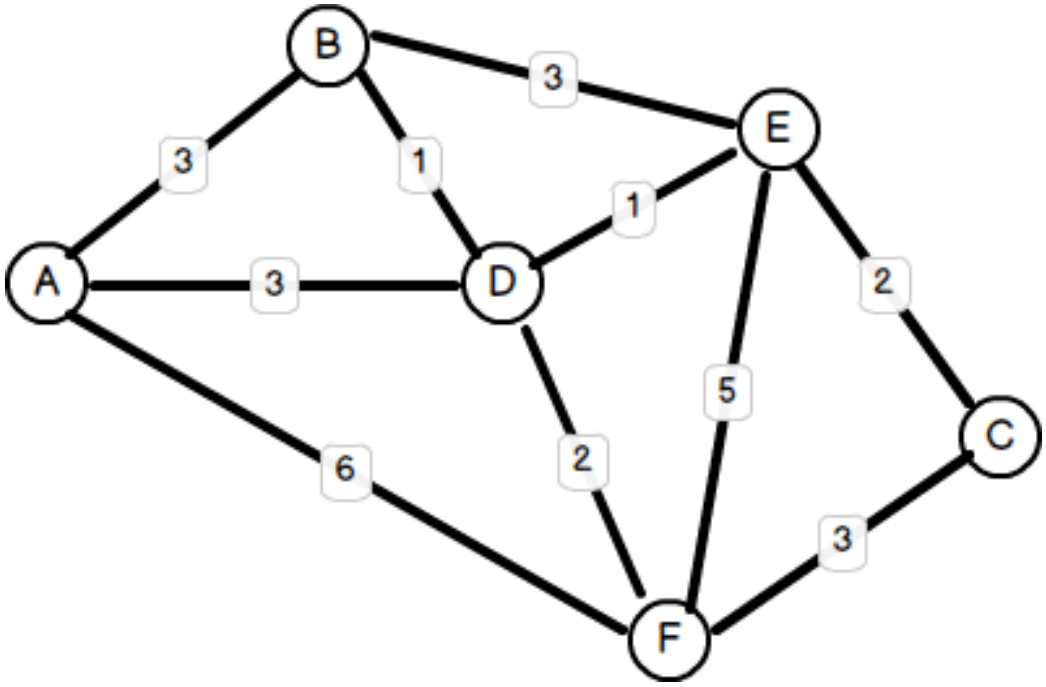


Figure 2.7 Weighed graph

The degree of a vertex v is denoted by $d_G(v)$ or briefly d(v) and is equal to the count of neighbors of vertex v. If the degree of vertex is 0, then it is isolated vertex.

The number $\delta(G)$ is the minimum count of edges incident to single node in G:

$$\delta(G) = \min\{d(v) \mid v \in V\}$$

The number $\Delta(G)$ is the maximum count of edges incident to single node in G:

$$\Delta(G) = \max\{d(v) \mid v \in V\}$$

If all the vertices of G have the same degree k, then G is k-regular, or simply regular. A 3-regular graph is called cubic. In Figure 2.4.[15,16, 17]:

- the degree of node 7 is d(7) = 2;
- the node 4 is isolated vertex d(4) = 0;
- $\delta(G) = \min\{d(v) \mid v \in V = \{1, \dots, 8\}\} = 0$;

- $\Delta(G) = \max\{d(v) \mid v \in V = \{1, \dots, 8\}\} = 3$;

A path is an elementary graph whose nodes are able to be organized in a linear arrangement in a such order that a pair of nodes are adjacent if they are consecutive in the arrangement and are nonadjacent any other way. In other word, a path is a non-empty single graph $P = (V_P, E_P)$, which form

$$V_P = \{x_0, x_1, \dots, x_k\}\ E_P = \{x_0x_1, x_1x_2, \dots, x_{k-1}x_k\},$$

where the x_i are all unrepeated. The nodes x_0 and x_k are associated by P and are called its ends; the nodes $x_1, \dots, x_{k-1}$ are the inner vertices of P [15,16, 17].

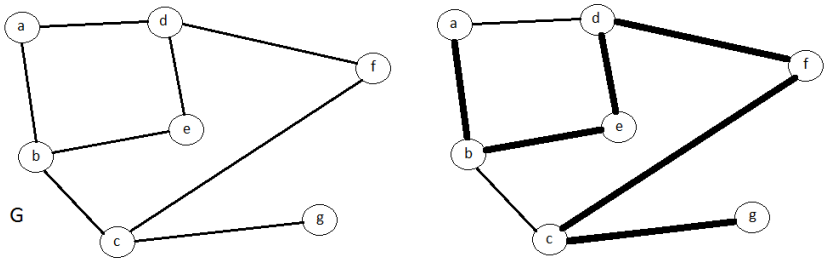


Figure 2.8 A path P = P^6 in G

A cycle on three or more nodes is a elementary graph whose nodes are able to be organized in a cyclic arrangement in a such order that a pair of nodes are adjacent if they are consecutive in the arrangement and are nonadjacent any other way. In other word, if $P = x_0 \dots x_{k-1}$ is a path and $k \geq 3$, then the graph $C = P + x_{k-1}x_0$ is a cycle.The length characteristic of a path or a cycle is the count of edges of appropriate part. A path or cycle with length k is termed a k-path or k-cycle, correspondingly. Depending on k a path or a cycle may be odd or even.Generally a 3-cycle is called a triangle, a 4-cycle a quadrilateral, a 5-cycle a pentagon, a 6-cycle a hexagon, and so on. Figure 2.9. illustrate a 3-path and a pentagon.

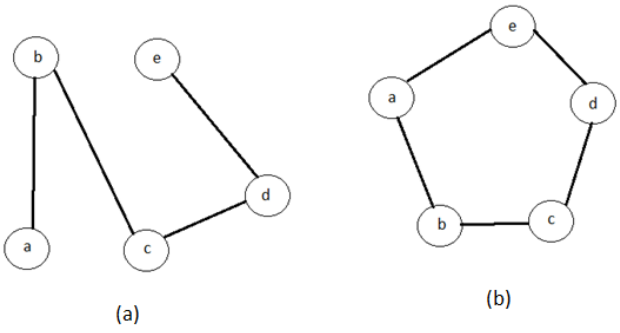


Figure 2.9 (a) A path of length three, and (b) a pentagon

A walk in a graph G is a sequence of vertices and edges such a W = v_0 e_1 v_1 ... v_{t-1} e_t v_t, where each pair of vertices v_{i-1} and v_i , $1 \leq i \leq t$ are neighbor and are the ends of e_i, $1 \leq i \leq t$. If v_0 = a and v_t = b, then W combine a to b and refer to Was an ab-walk. The a and b nodes of the W walk are the ends for this walk and they are called as initial vertex and terminal vertex, respectively. Apart from these nodes the other nodes are called v_1,...,v_t-internal vertices of theW walk. The t which is in the walk is stands for the length of the walk. Sometimes it is possible to label the walk as x-walk which means its initial node is x. If node does not have any repetitive nodes, then it is called trial walk. A walk is closed if v_0 = v_t. Otherwise it is open. In Figure 10 the walk W' = v_4 e_3 v_3 e_2 v_2 e_7 v_5 e_6 v_4 is closed. But the walk W = v_2 e_7 v_5 e_8 v_1 e_9 v_5 e_6 v_4 is open and also is trail [15,16, 17].

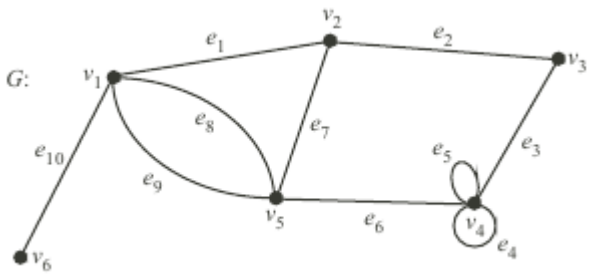


Figure 2.10 Connected graph

Two nodes u and v in graph G are connected if there is a uv-walk in the graph. If three nodes u, v and w in graph G, u and v are connected and v and w are connected, then u and w are also connected. If any two vertices are connected in non-empty graph G, then G is a connected graph. Graph in figure 2.6. is not connected. But graph in figure 2.10. is connected [16] [17].

A graph that contains no cycle is acyclic graph. Acyclic graph is a forest. Connected forest is a tree. The vertices of degree 1 in a tree are its leaves. Every non-trivial tree has at least two leaves. A tree with special vertex x is a rooted tree T(x). In rooted tree T(x) the vertex x called root of T tree. All possible trees with 6 vertexes are shown in Figure 2.11 [17].

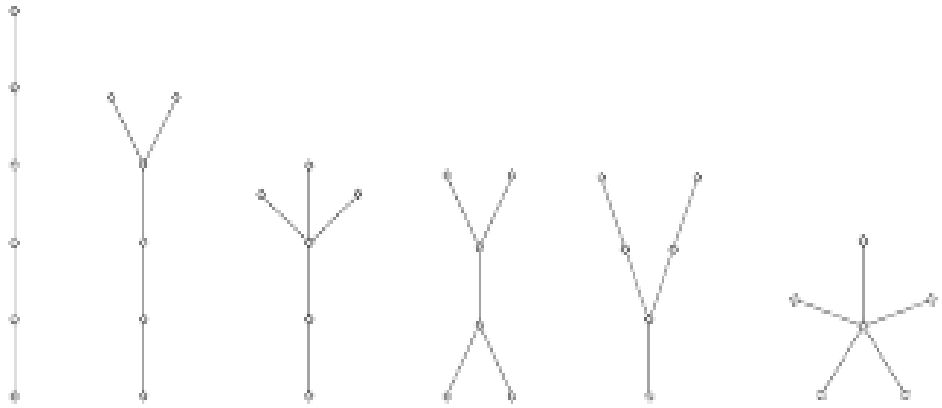


Figure 2.11 The trees on six vertices

If a subgraph T of a graph G is tree, then T is subtree of G. A subtree of graph G is spanning tree if it contains all vertices of G with minimum possible number of edges (Figure 2.12) [17].

-Spanning tree: Figure 2.12. shows a spanning tree of a graph in Figure 2.10. Let us assume the V vertices of the graph G=(V, E) has a vertices in clusters which is not empty and called N which again has a graph where any two nodes are not adjacent to each other. Then the cluster N which has these above mentioned characteristics is called independent set of the graph G [18].

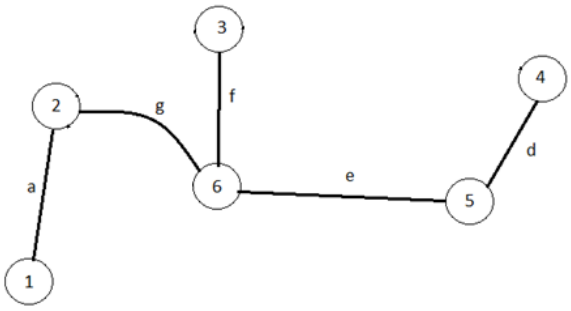
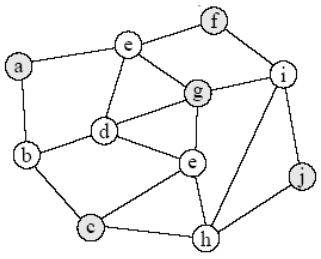


Figure 2.12 A spanning tree of a graph in Figure 10

An independent set of a subset of vertex set of the graph which generates an isolated subgraph of given graph. It is a maximal independent set of a graph that in independent set of the graph there is not such an element in vertex set of graph. This graph should be like when it is added to the independent set the condition of independency is not affected.A maximum independent set of a graph is maximal independent set of the graph with the largest number of vertices [18].



{a, d, i, h} is an independent set
{a, c, j, f, g} is a maximal independent set
{a, d, h, f} is a maximal independent set

Figure 2.13 Example of IS and MIS

The Independent Set problem is to find the maximum independent set in a graph. It is easy to find any independent sets. So that any single node is independent set, but it is problem to find maximum independent sets[17].

Consider a graph G = (V, E) and a subset D of vertex set V. A set D is called dominating set if each element of V is either in D or adjacent to any vertex in D. Minimum size of dominating set of vertices in graph G is called domination number of the graph G[17].

It is possible to have a conclusion that from the laws of maximal independent set and dominating set that every maximal independent set is also a dominating set. Nonetheless, the vice versa of it is not always true. Thus, every dominating set is not maximal independent set. Because elements of dominating set may be adjacent to each other [17].

Consider D is a dominating set of a graph G. Then each superset $D \subset D' \subset V(G)$ is also dominating set of a graph G. But subset of D is not always dominating set of graph G. If there is not any subset of D which is also dominating set, then D is minimal dominating set. A minimum dominating set of a graph is a minimal dominating set of a graph with least cardinality [17].

A dominating set D of graph G is a connected dominating set if D induces connected subgraph of G. Connected dominating set with minimum number of elements forms minimum connected dominating set [17].

The method of coloring is one of the most essential application areas of graph theory. When it is said vertex coloring of the G graph it is known as in some help of f accordance the cluster of V(G) vertices' elements are put against to any S cluster.That is to say, the cluster S elements are called colors. It is taking into account during these matchings that each point has to be only in one color and any neighbor nodes cannot be in the same color. If when the nodes of the graph G are colored, the k amount of colors are used then k is called colorable of graph G (figure 2.14). From this it is possible to come to the conclusion that the colorable k is separating the graph V(G) vertices cluster into independent sets color classes. Hence these independent sets are called color classes and f: $V(G) \rightarrow S$ is called color function.

The smallest number of the color which can be used in coloring the graph is called chromatic number of the graph or chromatic index of the graph and is symbolled as $\chi(G)$ [17].

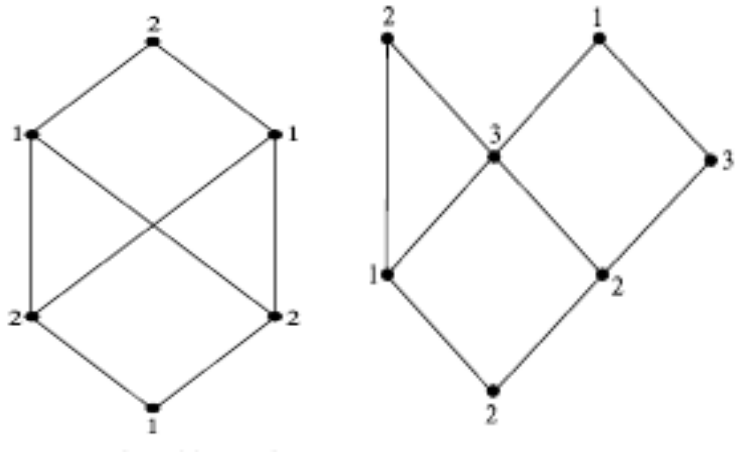


Figure 2.14 A 2-colourable and a 3-colourable graphs

2.4 Unit disk graph

Let's look at the set of n circles with equal radius in the plane. Each of equal-sized circles is disk which radius is one. Such kind of disk is called unit disk. The intersection graph of these unit disks is an n- is an edge between two nodes if and only if the Euclidean distance between such nodes is at most one i.e. u and v vertices is neighbor if and only if $|uv| \leq 1$ where | vertex graph. In such graph the vertex set of graph are the centers of unit disk. There uv| is the Euclidean distance between u and v. And it means at the same time that if v point is located at the control circle of the disk u and u point is located at control circle of disk v the u an v points are interconnected.The unit discs' connections graphs like these are called unit disk graph (Figure 2.15). [19, 20]

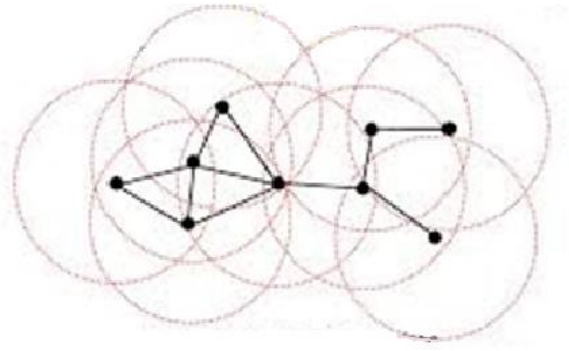


Figure 2.15 UnitDiskGraph

It is undeniable that for solving issues in the numerous real world problems for modelling the unit disk graphs are very helpful. In the unit disk graphs one of the most noticeable applications is possible to see in the wireless network field. In this field the unit disk graph characterizes an idealized multi-hop radio network. It is assumed that the nodes contain identical unit transmission radii and it is known that they are placed in the Euclidean plane. When they are in the mutual transmission range it is possible to have inter communication among them.Obviously, the behavior is carefully captured by the unit disk graph model. Thus, it is now a standard for the studies of ad hoc and sensor networks [21].

2.5 Set systems and projective plane. FP

2.5.1 Set system

In assumption that Y is definite known cluster. All the possible under clusters of this cluster is labelled as P(Y). Let us assume that $F \subset P(Y)$. Then, (Y, F) pair is called set system or design. And each element of the cluster Fis called block. In the set of (Y, F) system any element of the cluster Y which is degree of $u \in Y$, means how many time the u element is used at cluster F. If each of the elements of the cluster Yis used at the cluster F with the quantity of any r number, then this design is called r power regular design. The rank of (Y, F) set system is the length of the longest block of the cluster F. If length of the all blocks are equal to the same k figure, then this kind of design is called uniform of ran 3 design [22].

If at the system set of (Y, F) the cluster Y elements quantity is v, the cluster Fblocks quantity is b, the power of the set system is r and rank is k, then this kind of set system is called (v,b,r,k)-design. The main obligatory condition for having this kind of design existed is bk = vr equality [22, 23].

The any pair of the elements can use only λ amount of block which will becalled (v,b,r,k)-design (v, b, r, k, λ)-BIBD (balanced incomplete block design) [23].

2.5.2 Projective plane

A projective plane of order n ≥ 2 is an (n2 + n + 1, n2 + n + 1, n + 1, n + 1, 1)-BIBD. In the case of when n is a prime or a prime-powerthen a projective plane of order n exists [22].

For instance, if the prime number is equal to 2, so n = 2 then the projective plane (7, 7, 3, 3, 1)-BIBD is obtained. The table 1 is depicting its adjacency matrix [22].

Table 1: Adjacency matrix of projective plane (7, 7, 3, 3, 1)-BIBD

block	124	135	167	236	257	347	456
124	0	1	1	1	1	1	1
135	1	0	1	1	1	1	1
167	1	1	0	1	1	1	1
236	1	1	1	0	1	1	1
257	1	1	1	1	0	1	1
347	1	1	1	1	1	0	1
456	1	1	1	1	1	1	0

Chapter 3

WSN and Dominating Sets

Routing in infrastructure less wireless networks necessitates fast approach and low connection overhead. CDS is able to make a virtual backbone to network for packet routing and control. In dominating set based routing, also known as Backbone based routing information is able to route from starting node to adjacent node which is in dominating set, information moves through the CDS till the node in dominating set that adjacent to destination node, and finally to destination node.The major advantage of such routing is that the entire network is centralized into small connected dominating set [17] [24].

NP-complete is an issue of constructing a minimum CDS (MCDS) [25]. In the table 2 some algorithms were shown. There two categories such as Centralized and Distributed depending on the methods of algorithms used[17].

The lemmas mentioned below are used for constructing CDS.

Table 2. Comparison of the Presented CDS Algorithms

Algorithms	Type Time	Complexity	Message Complexity	Performance ratio
Marathe et al.	Centralized	-	-	10
Guha Khuller (1)	Centralized	-	-	2(1+H(Δ))
Guha Khuller (2)	Centralized	-	-	ln Δ +3
Ruan et al.	Centralized	-	-	3+ ln (Δ)
Wu et al.	Prune -based	$O(\Delta^3)$	Δ (n)	n/2
Chen et al.	Prune -based	-	-	-
Das et al.	Single Initiator	O(n2)	O(n2)	3H ( )
Wan et al. Single	Initiator	O(n)	O(nlogn)	8
Cardei et al.	Single Initiator	O(n)	O(n)	8
Cheng et al.	Single Initiator	O(n)	O(nlogn)	8
Kim et al.	Single Initiator	-	-	-

Zeng et al.	Single Initiator	O(n)	O(n)	7.6
Funke et al.	Single Initiator	O(n)	$O(n^2)$	6.91
Parthasarathy et al. (1)	Multiple Initiators	O($\log^2 n$)	O (n $\log^2 n$)	-
Parthasarathy et al. (2)	Multiple Initiators	O($\log^2 n$)	O(nlogn)	-
Li et al.	Multiple Initiators	O (Δ)	O(n Δ^2)	172
Cheng et al. (2)	Multiple Initiators	O(n)	O(n)	147

Lemma 1. There five independent vertices in the unit disc graph's vicinity (Figure 3.1.)[20].

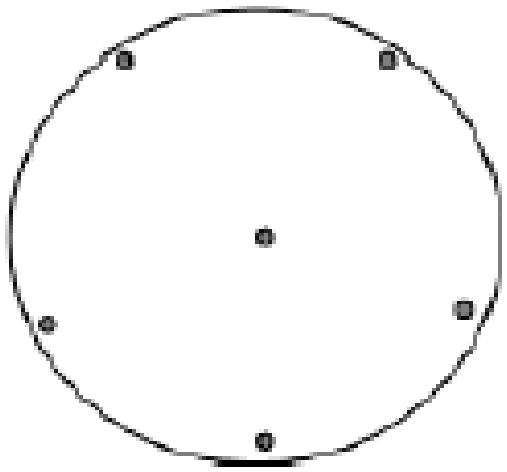


Figure 3.1 A Neighboring Area with 5 Independent Nodes

Taking into account that there are vertices namely, a, b, and c at the normal triangle which have unit edge length. Let us assume that a and b are connected via the arc which will have a radius at the center c, similarly, b and c are connected via a which has the radius center at a and finally the other two vertices are connected with the help of the third one with the radius center of it. Then, A is the area surrounded with these three arcs (Figure 3.2.).A is labelled as a unit arc-triangle of abc [20].

Lemma 2. It is not possible to have in a unit arc-triangle A two independent vertices [20].

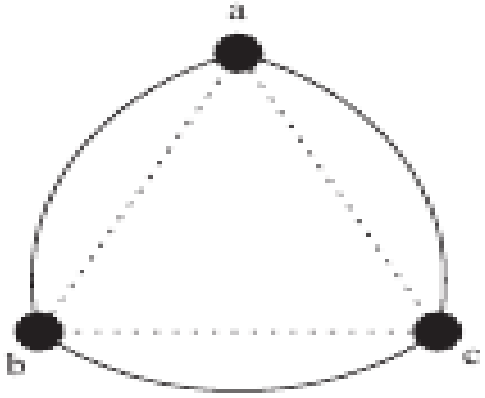


Figure 3.2 Unit arc-triangle abc

Lemma 3. The vicinity of two adjacent vertices have got maximum eight independent vertices [20].

Lemma 4. There minimum one spanning tree which every vertex will have at least five degrees for any unit disc graph [20].

Lemma 5. Each of the tree T which have minimum three vertices has a non-leaf vertex adjacent at maximum a non-leaf vertex [20].

3.1. Centralized Algorithms

-Marathe et al showed that Connected Domination (CDOM) algorithm in heuristic the vertex v was chosen arbitrarily as root. In every node for this MIS, the connecter will be requested to be added into NSi. The process itself continues from the deepest level to the peak level. At the end, all nodes which are located at IS as well as NS create a CDS. This ratio of performance is based on Lemma 1[17].

-Guha and Khuller showed that via labelling all the vertices white the first algorithm starts. Primarily, an algorithm chooses a node which has highest number of white neighbors. Then, the choose vertex is labelled as black while the neighbors of it are gray. When totally the vertices are labelled as gray as or black then the termination of algorithm takes place. The black nodes create altogether a connected dominating set[17].

3.2. Distributed Algorithms (Prune-based Algorithms)

-Wu et al at their studies showed that when the node has got two neighbors which do not have any connections between them then it is labelled as true. A connected dominating set was formed by the set of marked nodes (backbone or gateway nodes) (Figure 3.3)[17].

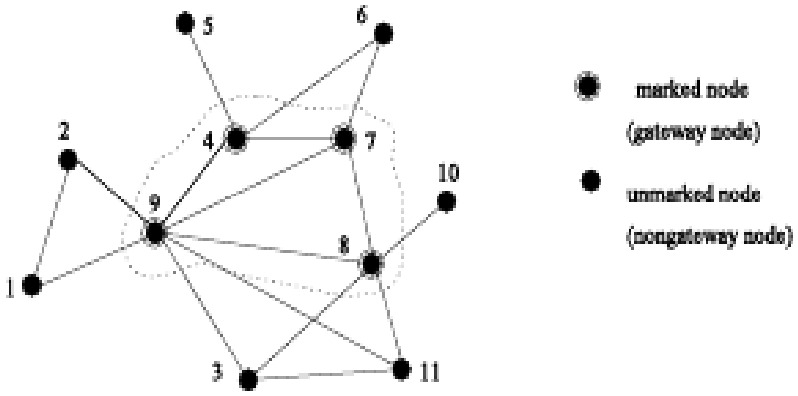


Figure 3.3 A Sampled Wireless Sensor Network

3.3. Distributed Algorithms (MIS-based Algorithms)

3.3.1. Single Initiator Algorithms

-Das et al said that;(i) Initially all nodes are colored white. (ii) The node which has the highest node degree is nominated as root. Then it is colored with black, whereas, its neighbors are gray colored. (iii) Choose the gray node which is white neighbors' quantity ifs the highest (Figure 3.4.) [17].

-Wan et al proposed the single Initiator algorithm. Firstly, by utilizing distributed leader election algorithm the root is selected simultaneously the spanning tree was built. The CDS was created by the all nodes at dominating tree (Figure 3.5)[17].

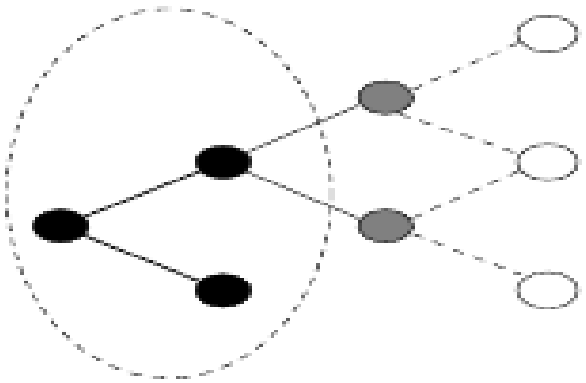


Figure 3.4 Black Nodes Connected Dominating Set (CDS)

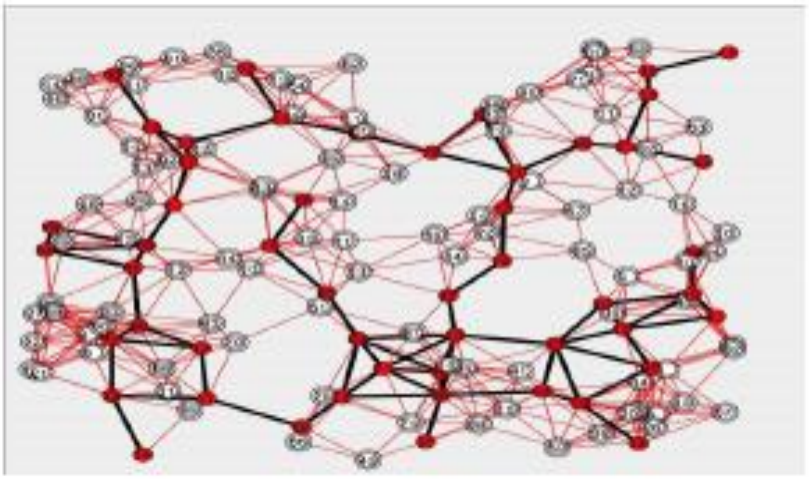


Figure 3.5 A Wan et al., Backbone

-Cheng et al presented that without depending on the spanning tree at the leader the first algorithm will grow and together will created a CDS with non-leaf nodes[17].

-Kim et al offered the idea that a Timer-based Energy which are in the other word CDS algorithm are Connected Dominating Set protocols. The mentioned algorithms have got two phases, namely, the first phase an initiator which is base is order pair like energy and degree or degree and energy and the second phase called dominator [17].

3.3.2. Multiple Initiators Algorithms

-Parthasarathy et al two distributed algorithms suggested in which the first had three steps. The first phase involved by utilization of the list of c colors coloring D2 nodes. Once it is done, in the network all the nodes contained a valid D2-coloring. At the second phase a MIS is constructed. Here during the slot i all nodes which were at the color i tried to link the MIS. The third phase contains more node exchange process. Thus, here MIS nodes shared and received their data among all three-hop neighbors via utilization of messages PHASE-1 and PHASE-2. The key idea for the second algorithm is same like the main idea for the first algorithm. Nevertheless, the first algorithm utilized D2-coloring in order to have a reduction in the collision [17].

-Cheng etal said that in this algorithm, the node which has the lowest ID convertsinto a MIS node that is marked as red. Next, the node transmits into black

once it does not have any red node domination. Hence, all red and black nodes create the MIS. The connectors are specified too once, maximum two of the hop neighbors changed the information they had. Various colors were used for various connectors[17].

Chapter 4

In this section our aim is utilizing dominating set and other corresponding subsets in graph theory which display an independent, far reaching treatment in utilizations of virtual backbone (VB) foundation and topology control in WSNs. In DSN there is no physical spine foundation, a VB can be framed by building a CDS. The CDS of a chart speaking to a system significantly affects an effective plan of routing security calculations in WSN[22].

Wireless sensor network (WSN) is made out of numerous miniaturized scale sensor nodes which can gather, store and process ongoing natural data, forward the outcomes to its clients. Sensor nodes are appropriated to the objective range in vast numbers and their area inside this region is resolved randomly. Sensor nodes may be useless and fresh sensor nodes might be throw in to the system. WSN is regularly sent in cruel condition, unmanned regions or foe zone. Since sensor nodes are sent in unattended designs or even in threatening situations, they can promptly be caught and altered by enemies and additionally correspondence joins are traded off. Secure correspondence among sensor nodes requires validation, protection and honesty, along these lines for secure correspondence between two sensor nodes a mystery key is required and cryptographic key administration is a testing errand [22].

The keys put away into ROMs of sensors must be precisely chosen. With the goal that two neighboring sensor nodes have no less than one key in like manner. Along these lines, in sensor networks, mystery key sharing is the establishment and center. On the off chance that there is no impeccable key pre-conveyance conspire, information encryption, information validation and personality confirmation won't be guaranteed. Consequently, combine astute key foundation is essential in the method for accomplishing ideal versatility to limit a traded off range to one-bounce separate just [26].

The vast majority of the DSNs utilize the symmetric key schemes in light of the fact that these plans devour less calculation time than asymmetric schemes. Since sensor nodes convey restricted power sources, our concentration is over symmetric

key pre-distribution plans. One of significant worries in the sensor network applications is the way the secrecy of the detected information and the control message traded among sensor nodes can be ensured [22].

Key pre-distribution schemes (KPSs) divided into 3 stage: key pre-distribution, shared-key disclosure and path key foundation. In the key pre-distribution stage, a vast pool of keys and their key identifiers are produced. Each sensor nodes are stacked with a settled number of keys looked over the key pool, alongside their key identifiers. After arrangement of the DSN, the mutual key revelation stage happens, where two hubs in remote correspondence extend search for their regular keys. In the event that they share at least one normal keys, they can pick one of them as their mystery key for cryptographic correspondence. The path key foundation stage happens if there is no basic key between a couple of nodes in a wireless correspondence range. At that point, they search for different secure connections to achieve other, so that one of them can pick a subjective key and after that transfer it through the connections in encoded shape to the goal node [22].

It is possible to use one of the three approaches for solution of key pre-distribution problem [27]:

- probabilistic,
- deterministic,
- hybrid.

In probabilistic arrangements, key-chains are arbitrarily chosen from a key-pool and disseminated to sensor nodes. In deterministic arrangement, deterministic procedures are utilized to plan the key-pool and the key-chains to give better key network. At last, half and half arrangements utilize probabilistic methodologies on deterministic answers for enhance adaptability and flexibility [22].

The normal approach is to dole out every sensor node various keys, arbitrarily drawn from a key-pool, to develop a key-chain to guarantee that either two neighboring nodes have a key in like manner in their key-chain, or there is a key-path. Along these lines the test is to settle on the key-chain size and key-pool estimate so that each match of nodes can set up a session key straightforwardly or

through a path. Key-chain estimate is constrained by the capacity limit of the sensor nodes. Besides, little key-pool builds the likelihood of key offer between any match of sensor hubs by diminishing the security in that, the quantity of the keys should have been found by the enemy diminishes. Correspondingly, extensive key-pool diminishes the likelihood of key offer by expanding the security [22].

WSNs can be demonstrated as unit disk graph [28], where two nodes are adjacent on the off chance that they are inside each other's transmission extend. Deterministic and combinatorial approach has solid focal points over the randomized one. With the best possible outline of BIBD, for example, projective plane, we can guarantee the full network of key pre-dispersion plot. Hindrance of this arrangement is that, parameter n must be a prime power; subsequently, not all system sizes can be upheld for a settled key-chain measure. Different arrangements have been proposed to address this restrictions [22].

1. generalized quadrangles (GQ)
2. hybrid design;

In a DSN for a KPS it is possible to use an uniform and regular set system $(Y,\mathbb{F})$.

Example 1. Assume that $Y = \{ y_i : i = \overline{1,v} \}$ and $F = \{F_j : j = \overline{1,b} \}$. Give the sensor nodes a chance to be indicated $n_1,\ldots,n_b$ which recognize the b blocks in $\mathbb{F}$. Further, the elements in Y are related to an arrangement of v keys, as a key q_i , $1 \leq i \leq v$ is arbitrarily browsed some predefined key-space. At that point, the sensor node n_j , $\overline{1,b}$ gets the arrangement of keys which are in block F_j: $\{ q_i : y_i \in F_j \}$. The block F_j helps to indicate which keys are identified to the node n_j. It is helpful and advantageous if each node gets a consistent number of keys and each key is allotted to a steady number of sensor nodes [23].

Due to example given above, let introduce following definition:

Definition. Two nodes n_r and n_t share joint key if and only if $F_r \cap F_t \neq \emptyset$ where F_r and F_t are blocks of appropriate nodes [22].

4.1 One-hop and multi-hop connections in set system.

4.1.1One-hop local connections

Lemma 1. Any vertex (block) F_j in the block graph $G_{\mathcal{F}}$ of a (v, b, r, k)-design, (Y, $\mathcal{F}$), has degree at most k(r – 1). Further, all vertices in $G_{\mathcal{F}}$ have degrees equal to k(r – 1) if and only if $|F_i \cap F_j| \leq 1$ for all $F_i, F_j \in \mathcal{F}$, $i \neq j$ [23].

Lemma 2. (v, b, r, k, λ)-BIBD exist only if λ(v – 1) = r(k – 1) and bk = vr and b ≥ v [23].

Let now show that, we can use a projective plane with order $n \geq 2$ for KPS: ($n^2 + n + 1$, $n^2 + n + 1$, $n + 1$, $n + 1$, 1)-BIBD. Design bolsters n^2+n+1 nodes, and utilizations key-pool of size $n^2 + n + 1$. It creates $n^2 + n + 1$ key-chains of size $n + 1$ where each match of key-chains has precisely one key in like manner and each key shows up in precisely $n + 1$ key-chains. After the sending, each match of nodes finds precisely one normal key. Accordingly, likelihood of key sharing among a couple of sensor node is 1 [22].

Theorem 1. Assume that p is a prime or a prime power. At that point there exists a KPS for a DSN having $p^2 + p + 1$ nodes, in which each node gets precisely $p + 1$ keys, and in which any two nodes share precisely one key [22].

The plans of Theorem 1 may be consummately appropriate for little DSNs.

Example 2. If we take p = 29, we can get a DSN on 871 nodes in each node can gets 30 keys.

Notwithstanding, for extra huge DSNs, the capacity prerequisite may be too enormous. For example, for 20000 nodes storage requirement is 150 [22].

4.1.2 Multi-hop connections

If $G_{\mathcal{F}}$ is not a complete graph, then it has a probability that two nodes n_r and n_t in closeness does not have a common key. For this situation, the two nodes n_r and n_t can convey through a 'two-jump way' gave that there is a node n_c which is adjacent to both n_r and n_t such that $n_r \cap n_t \neq \emptyset$and $n_r \cap n_t \neq \emptyset$ [22].

4.2 Projective plain disadvantages

In the first place disadvantage of projective plain model is that in substantial network systems are confronted with the issue of memory restriction which we described above. Second inconvenience of this model is about parameter n which must be prime number or prime power. Along these lines, the sensor network can't bolster discretionary system sizes [22].

Two approaches have been requested to cure these disadvantages [22]:

4.2.1 Generalized quadrangles (GQ)

GQ: by utilizing GQ design within the property which not all couples of adjacent nodes are possible to share a key specifically. In GQ, a couple of key-chains might not have a key in like manner, but rather GQ ensures that there are another key-chains that share precisely one key with all them. A limited GQ is a frequency structure S = (P, B, I) where P and B are disjoint and non-exhaust sets of points and lines, separately and for which I is a symmetric point-line rate connection fulfilling the accompanying axiom [22]:

1. every points are episode with t + 1 lines ($t \geq 1$) and two particular points are occurrence with at most one line

2. each line is episode with s + 1 points ($s \geq 1$) and two particular lines are occurrence with at most one point

3. on the off chance that x is a point and L is a line not occurrence (I) with x, at that point there is a novel match $(y, M) \in P \times B$ [22].

Assume GQ(s, t) = GQ(q, q) where lines are indicate blocks and points indicate objects. Therefore, there are $v = b = (q + 1)(q2 + 1)$ blocks and objects in which each block encompasses $s + 1 = q + 1$ objects, and where each object is encompassed in $t + 1 = q + 1$ blocks [22].

In spite of the fact that GQ is more versatile than symmetric design, parameter n still should be a prime power [22].

4.2.2 Hybrid designs

Given a coveted number of sensor nodes which is similar to a coveted number of keys in the pool, we will be unable to build a combinatorial plan for the objective

parameters. By utilizing symmetric or GQ plan and its supplement, this plan jelly pleasant properties of combinatorial outline yet take preferences of adaptability and versatility of probabilistic ways to deal with help any system sizes [22].

Assume a sensor network with n nodes. In this case n key-chains are needed. Because of memory restrictions, key-chains could store maximum K keys originating from key-pool P. We are able to utilize hybrid design in order to the situations where there is not any familiar combinatorial design strategy to produce design including N nodes for the given key-chain estimate K. Essentially, hybrid configuration finds biggest prime power n with the end goal that $k \leq K$ and produces N blocks of size k in which objects originated from set S which size is $|S| = v$. The b number of N blocks are produced by major symmetric or GQ design and N – b blocks are haphazardly chosen among k-subsets of the corresponding design blocks. Given a block design $D = (v, k, \lambda)$ along a set S with v objects and $B = B_1, B_2, \ldots, B_b$ of $|B| = b$ blocks where every blocks incorporate precisely k objects, complementary design $\overline{D}$ has the complement blocks $\overline{B_i} = S - B_i$ as its blocks for $1 \leq i \leq b$. $\overline{D}$ is a block design with parameters $(v, b, b - r, v - k, b - 2r + \lambda)$ where $(b - 2r + \lambda > 0)$. If $D = (v, k, \lambda)$ is a symmetric design, then $\overline{D} = (v, v-k, v-2r + \lambda)$ is also a symmetric design [22].

Still hybrid design described as a complementary method which ensure that the technique applies to the system with discretionary size, it has as yet one concern: the capacity overhead [22].

4.3 Key copying and exchanging (KCAE)

In this subsection we will look through an effective and secure technique for topology control and deterministic KPS by KCAE with making virtual backbone for distributed wireless sensor networks. Sensors utilize disconnected key pre-distribution with projective plain and after that online key-chain circulation after sending in the system by dominators group (DG) sensors. Our plan works with the idea of CDS to diminish memory space, increment network adaptability and takes after SBIBD scheme and projective plane. The sort of expected administrations from WSNs has been built up in light of the dependable information transmitting that

steering and proficiency of the system incorporates some security components. In our approach, we will offer a plan for key conveyance and trading among sensors that repairs inconveniences of the projective plane scheme [22].

We will utilize CDS along the system for reaching our goal. Our motivation is to make sure about the security and change in SBIBD configuration drawbacks in the system so a little arrangement of dominator nodes can cover the entire system safely. We consider that dominator nodes are totally secure and the assailant couldn't have any impact them in any capacity. Our investigation and reenactments demonstrate that our plan (KCAE) can supply security of appropriated sensor organize in ideal state [22]

4.3.1 Model

As discussed above we can research topology of entire DSNs as a UDG [28]. Dominated nodes connect to dominators with one hop communication. Correspondences among dominator nodes make one virtual backbone for the network system on the grounds that the entire information transmission is simply by dominator nodes. But dominated nodes could in no way convey among each other and every one of the sensors are the same. Keeping in mind the end goal to frame a protected system it is important to apply a two phase operation [22]:

1 key copying

2 stage key trading.

Assumption 1: sensors are settled in their position in the wake of being conveyed.

Assumption 2: in one unit disk or radio scope of one sensor, all the adjacent sensors don't really have coordinate correspondence joins among each other aside from virtual backbone connection [22].

4.3.2 Key copying

Sensors accept their key-chain through projective plane on key pre-distribution scheme. Let separate the sensors set V into two subsets of (V1, V2); where V1 is dominators group (DG) sensors and V2 is dominated sensors (DS).

The set of V_2 is itself separate into subsets of w_i, $i = \overline{1, N}$; where N is at most possible subsets of V_2. Every w_i will be allocated on one part of V_1. We demonstrate sensors inside subset w_i by (DS_1, DS_2,…,DS_η) which make concessions with one sensor from V_1 that is denoted by (DG_i, i = 1,2,…, $\gamma_c(G)$) (Figure 4.1) [22].

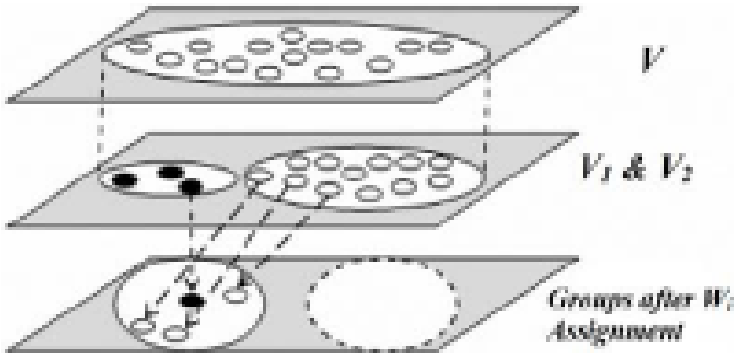


Figure 4.1DSS membership in DGS

Assumption 3: discharge nodes incorporates one arbitrary session key from which it connects with DGs in its radio range (DG1hop) and gets its key or DG1hop duplicates key to that void node [22].

Assumption 4: Every sensor has same radio range.

Assumption 5: dominator nodes incorporate n + 1 key with least cover on the one key and can utilize their neighbor dominator nodes and subsets of w_i to duplicate keys in purge nodes [22].

Assumption 6: the quantity of nodes in one group (η) is settled on request and η is indeed at most degree of DGs in each group, in fact; $\eta = (\Delta(DG_i))$ [22].

4.3.3 Network formation

After defining of dominating number $\gamma_c(G)$ or the quantity of dominator sensors and the measure of η for each group, one key pre-distribution along design ($n^2 + n + 1$, $n^2 + n + 1$, n + 1, n + 1, 1)- BIBD is done and in the event that we pick the quantity of sensors fancied and demonstrate it by the parameter of N, we create network versatile, at that point least $n^2 + n + 1$ nearer to N will be accomplished ($n^2 + n + 1 \leq N$) and formulate the above projective plane. In the example threeit is depicted in Figure 4.3., that; $\eta = 2$ and $\gamma c(G) = 3$. Discharge nodes ($N - (n^2 + n + 1)$) are disseminated in nature just by one randomized or fancied session key. Likewise, we

consider that the quantity of sensors is so huge and the key keeping space in each node is extremely constrained, i.e., this time the quantity of keys and key-chain are picked sought and restricted, for this situation; base on the number existing keys that is demonstrated by the parameter N', minimal measure of n2+n+1 is nearer to N', (n^2 + n + 1 ≤ N') and projective plane (n^2 + n + 1, n^2 + n + 1, n + 1, n + 1, 1)- BIBD is established. Discharge nodes (N' – (n^2 + n + 1)) are circulated in the nature just by one randomized or sought session key [22].

• When the nodes are sending an encrypted request for connections to the groups the try to find their DG1hop. DG1hop meanwhile directs its key chain via replying to the request like encrypted as well as by acting like to the node like its member [22].

• There some circumstances when the empty node will not have same session key like its dominator, DG1hop. In this case the dominator node sends the received packet to the dominator which is located in the neighborhood. Nonetheless, sometimes even this neighbor dominator does not have any common key with the node so it forwards the received packet to its neighbor dominator. This actions continuous until the same key is reached [22].

In the figure 4.2. (a) Key pre-distribution with network size n = 9 by projective plane (7, 7, 3, 3, 1)-BIBD depicted, while, randomized session keys in key copying was shown in the figure 4.2 (b) [22].

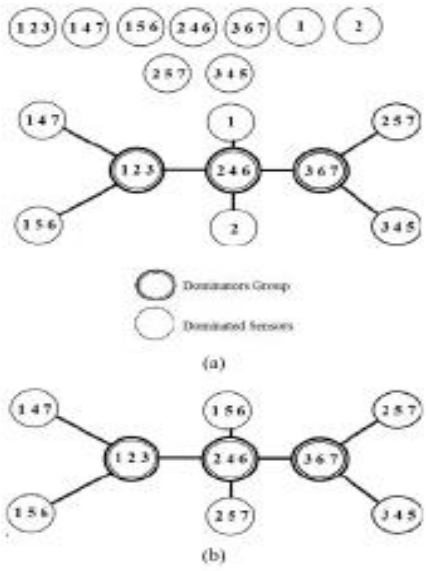


Figure 4.2 Randomized session keys

4.4 Key exchanging

In order having key pre-distribution the projective plane was properly utilized. It means that the dominators must have same key like all the sensors at the all groups. By using the randomized cryptography keys, the logical model application provides us with the secure deliveries of the messages in the network. In the figure 4.3. the pseudo-code for this algorithm is depicted [22].

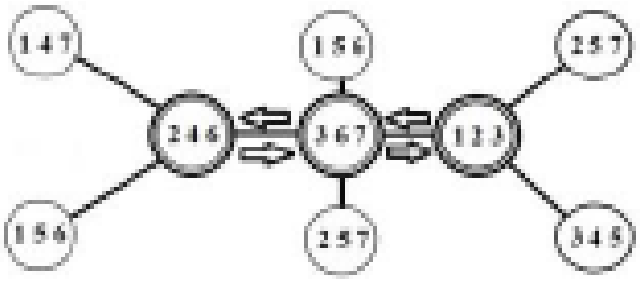


Figure 4.3 Key exchanging between DGS

CHAPTER 5

CONCLUSION

In this thesis our main aim was to explain the use of WSN technology in the modern and clever environment with the high efficiency in order to provide the safety and security. That was the reason why in the beginning of the thesis work the main focus was on the giving some information about WSN itself. Due to the restrictions on the WSN such as energy, processing and memory limitations unlike from other wireless systems creates additional challenges. Thus we are not able to apply general security methods into the WSN because of these restrictions which leads us to specially generate and create new topology control methods for WSNs. In order achieving that we approached to the theory of graphs which has been widely applied in the network systems. In the base of the connected dominating set which were discussed at the theory of graphs the topology control was created. In the topology control it has been designed that the connections at the WSN are not at the all nodes but only at the nodes which are located at the dominators. Thus, by doing so the additional useless connections among the nodes of the WSN is reduced. Next to it, the centralized and distributed algorithms were studied for creating CDS. During the research it was shown that the length of the CDS which was created with centralized algorithm was less than the length of the CDS which was created with the distributed algorithm. Moreover, the topology of whole network has to be informed before for these types of centralized algorithms. In the big scale WSNs the distributed algorithms are more suitable. Hence, these kinds of algorithms are very effective in terms of power and time.

Once info about the CDS algorithms was given, a strong technique about control of topology at WSN in consideration of deterministic key pre distribution together with combinatorial projective plain plan by KCAE using of CDS is shown. The suggestion was KCAE alongside to CDS in order to achieve key distributions for any system at any size. Similarly, the principle which we focused on in our studies was dominator nodes as well as sensor grouping in DSN with VBs. After an

examination and correlation computationally it has been clear from the demonstrations that the combinatorial KCEA has effective points of interest such as:

1) It hardly ever possible not to have common key between any two sensor nodes
2) By providing scalability with the help of the CDS algorithms the length of the key path is reduced
3) It increases the probability of security at connections.

References

1. https://en.wikipedia.org/wiki/Wireless [Last Accessed on 25th of June 2017]

2. John Ross, "The Book of Wireless, 2nd Edition: A Painless Guide to Wi-fi and Broadband Wireless"

3. Prashant Tiwari, Varun Prakash Saxena, Raj Gaurav Mishra, Devendra Bhavsar, "Wireless Sensor Networks: Introduction, Advantages, Applications and Research"

4. " 21 ideas for the 21st century " , Business Week, Aug. 30 1999, pt. 78 – 167

5. M.A. Matin and M.M. Islam, "Overview of Wireless Sensor Network"

6. José Cecílio, Pedro Furtado, "Wireless Sensors in Heterogeneous Networked Systems: Configuration and Operation Middleware"

7. Fabian Nack, "An Overview on Wireless Sensor Networks"

8. Michael Healy, Thomas Newe and Elfed Lewis, "Wireless Sensor Node Hardware: A Review"

9. Sanjeev Kumar Gupta, Poonam Sinha, "Overview of Wireless Sensor Network: A Survey"

10. AmitSarkar, Senthil Murugan, "Routing protocols for wireless sensor networks: What the literature says?"

11. Jamal N. Al-Karaki, Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey"

12. George S. Oreku, Tamara Pazynyuk, "Security in Wireless Sensor Networks"

13. Fei Hu, Jim Ziobro, Jason Tillett, Neeraj K. Sharma, "Secure Wireless Sensor Networks: Problems and Solutions"

14. https://simple.wikipedia.org/wiki/Seven_Bridges_of_K%C3%B6nigsberg [Last Accessed on 25th of June 2017]

15. J.A. Bondy U.S.R. Murty, "Graduate Texts in Mathematics Graph Theory "

16. Reinhard Diestel, "Graph Theory"

17.Amir Hassani Karbasi and Reza Ebrahimi Atani, "Application of Dominating Sets in Wireless Sensor Networks"

18. Gabriel Valiente, "Algorithms on Trees and Graphs"

19. David S. Johnson, Brent N.Clark And Charles J. Colbourn, “Unit Disk Graphs”
20. Weili Wua, Hongwei Du, Xiaohua Jia, Yingshu Li, Scott C.-H. Huang, Minimum connected dominating sets and maximal independent sets in unit disk graphs”
21. Fabian Kuhn, Thomas Moscibroda, Roger Wattenhofer, “Unit Disk Graph Approximation”
22. Amir Hassani Karbasi and Reza Ebrahimi Atani, “Projective plane-based key pre-distribution by key copying and exchanging based on connected dominating set in distributed wireless sensor networks”
23. Jooyoung Lee, Douglas R. Stinson, “On the Construction of Practical Key Predistribution Schemes for DistributedSensor Networks Using Combinatorial Designs”
24.Jie Wu and Hailan Li, “On Calculating Connected Dominating Set for Efficient Routing in Ad Hoc Wireless Networks”
25.Michael R. Garey, David S. Johnson, “Computers and Intractability: A guide to the theory of NP-completeness”
26. Lidong Zhou and Zygmunt J. Haas, “Securing Ad Hoc Networks”
27. Seyit A. Camtepe and Bulent Yener, “Key Distribution Mechanisms for Wireless SensorNetworks: a Survey”
28. M.V. Marathe, H. Breu, H.B. Hunt, S.S. Ravi, D.J. Rosenkrantz, “Simple Heuristics for Unit Disk Graphs”